The Complete Internet Security Manual

Expert Tutorials to Improve Your Skills

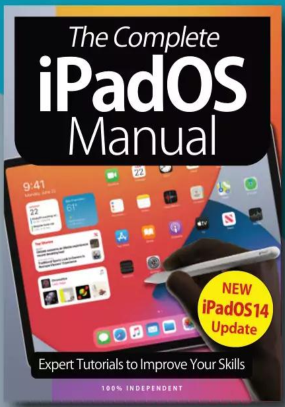
100% INDEPENDENT

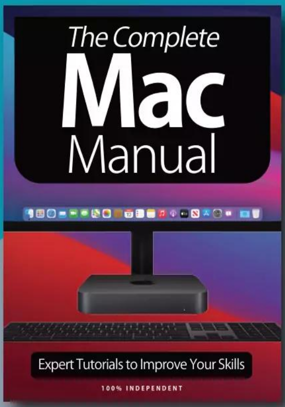
VISIT…

LANZAROTE
Caliente.COM

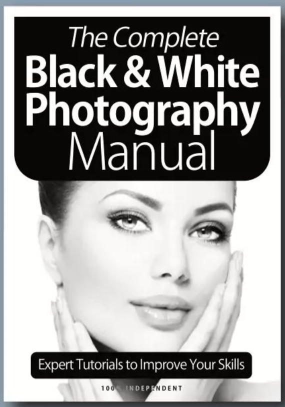
Discover more of our guides today...

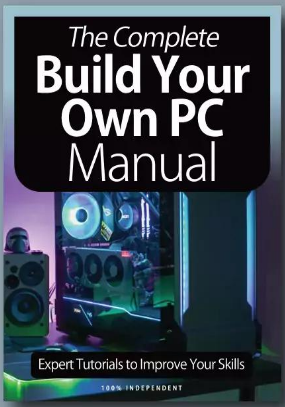
The Complete
iPhone
Manual
NEW iOS 14 Update
Expert Tutorials to Improve Your Skills
100% INDEPENDENT

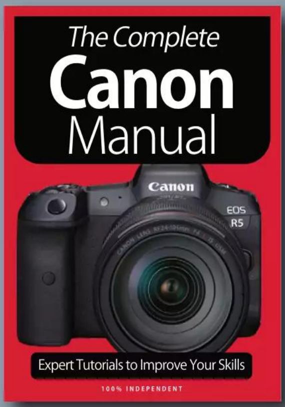

The Complete
iPadOS
Manual
NEW iPadOS 14 Update
Expert Tutorials to Improve Your Skills
100% INDEPENDENT

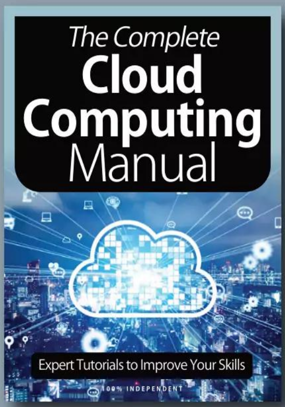

The Complete
Mac
Manual
Expert Tutorials to Improve Your Skills
100% INDEPENDENT

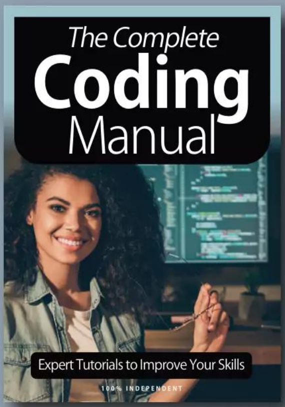
The Complete
Android
Manual
Expert Tutorials to Improve Your Skills
100% INDEPENDENT

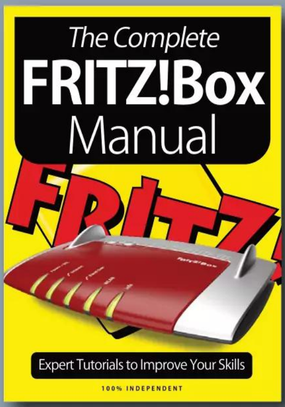

The Complete
Black & White Photography
Manual
Expert Tutorials to Improve Your Skills
100% INDEPENDENT

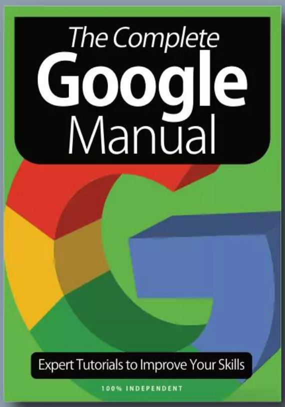

The Complete
Build Your Own PC
Manual
Expert Tutorials to Improve Your Skills
100% INDEPENDENT

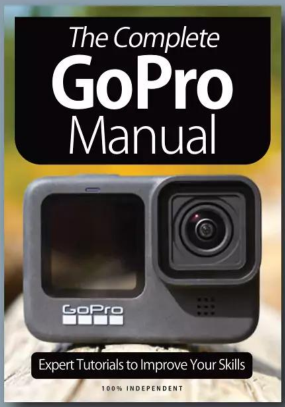

The Complete
Canon
Manual
Canon
EOS R5
Expert Tutorials to Improve Your Skills
100% INDEPENDENT


The Complete
Cloud Computing
Manual
Expert Tutorials to Improve Your Skills
100% INDEPENDENT


The Complete
Coding
Manual
Expert Tutorials to Improve Your Skills
100% INDEPENDENT

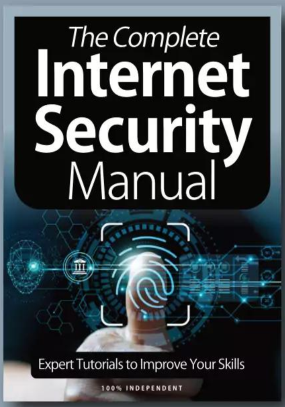

The Complete
FRITZ!Box
Manual
FRITZ!
Expert Tutorials to Improve Your Skills
100% INDEPENDENT

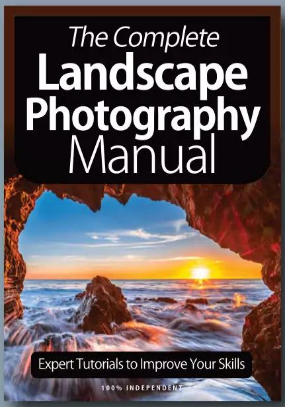

The Complete
Google
Manual
Expert Tutorials to Improve Your Skills
100% INDEPENDENT


The Complete
GoPro
Manual
GoPro
Expert Tutorials to Improve Your Skills
100% INDEPENDENT

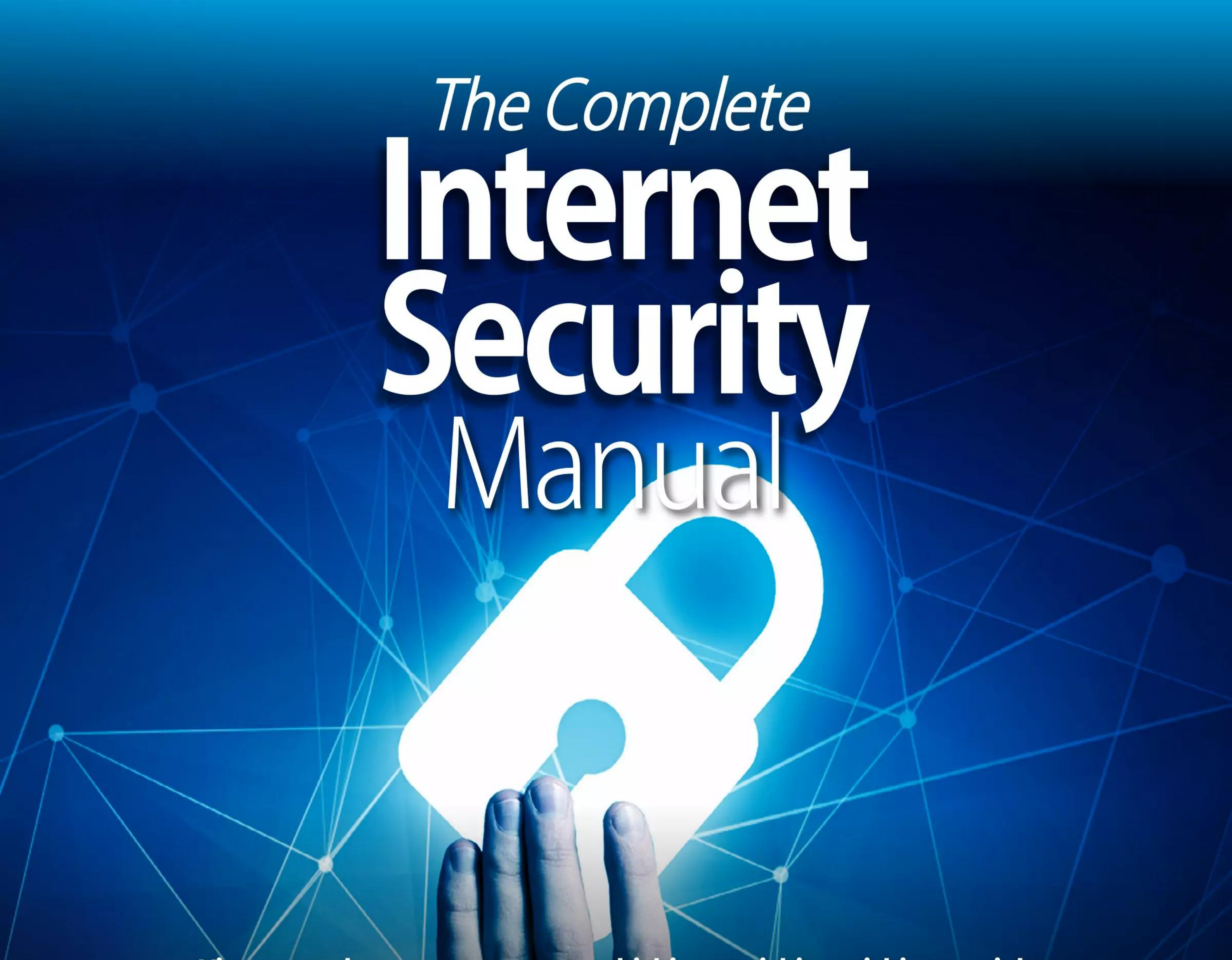
The Complete
Instagram
Manual
Expert Tutorials to Improve Your Skills
100% INDEPENDENT

The Complete
WhatsApp
Manual
Expert Tutorials to Improve Your Skills
100% INDEPENDENT


The Complete
Internet Security
Manual
Expert Tutorials to Improve Your Skills
100% INDEPENDENT


The Complete
Landscape Photography
Manual
Expert Tutorials to Improve Your Skills
100% INDEPENDENT

The Complete Internet Security Manual



Viruses, malware, ransomware, phishing, smishing, vishing, social engineering… the list of digital threats with peculiar names expands daily and hardly a moment goes by without some form of attack appearing in the news. We live in interesting times, where data is worth more than oil or gold and your personal information is greatly sought after by cybercriminals, scammers and hackers. How prepared are you for this new age of digital vandalism and theft? Is your Windows 10 computer secure against the continual onslaught of the modern online world? We'll help you secure your computer, network and devices against such threats and with easy to follow tutorials, help arm you against potential threats and attacks. For parents and guardians, we also cover looking out for your children when online, together with guides on how best to protect them and advice from industry experts. You'll soon be security savvy and prepared for whatever digital threat looms on the horizon.

@bdmpubs BDM Publications www.bdmpublications.com

Contents

8 Modern Day Security

10 Types of Security Risk
12 Hackers and You
14 Social Engineering
16 Ransomware: How it Works
18 The Virus Top Ten
20 Phishing, Vishing and Smishing
22 Pharming
24 Windows 10 Security
26 Digital Security FAQ

28 Protecting Yourself

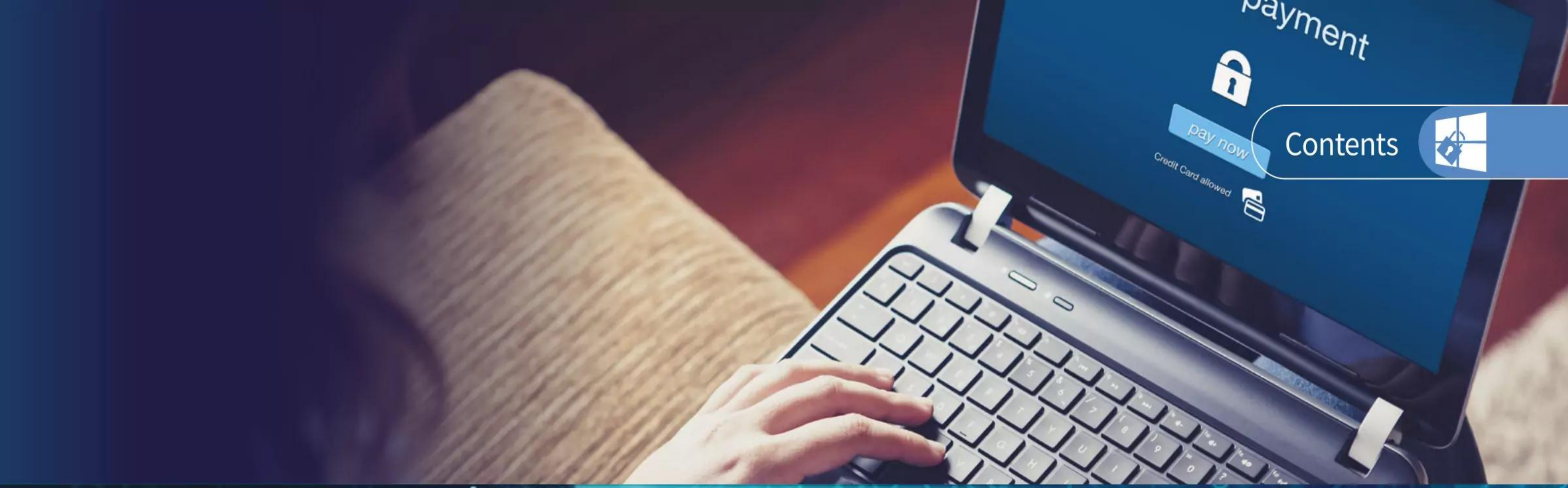
30 Be Smart
32 Top Ten Antivirus and Security Packages
34 Bitdefender Total Security 2018 Review
36 Kaspersky Total Security 2018 Review
38 McAfee Total Protection Review
40 Setting Up Windows 10 Security
42 Why Updating is Important
44 What to Keep Updated and How
46 How to Secure Your Web Browser
48 How to Secure Your Home Network
50 What are Wireless Security Standards?
52 How to Secure Your Wireless Network
54 What is Encryption?
56 Encrypting Your Windows 10 Laptop
58 Top Ten Encryption Tools for Windows 10
60 What is a VPN?
62 How Can a VPN Improve Windows Security?
64 Top Ten VPNs
66 Using a VPN for Added Security and Privacy

68 Online Protection & Disaster Recovery

70 How Does Information Move Around the Internet?
72 How Can Internet Data be Intercepted?
74 10 Tips to Protect Yourself Against Interception
76 How to Secure Your Devices
78 How to Secure Yourself on Facebook
80 How to Secure Yourself on Twitter
82 How to Secure Yourself on WhatsApp
84 What to Avoid when Creating a Password
86 Password Generators and Tools
88 Top Ten Password Managers
90 Shopping Online and Security
92 How to Remove a Virus or Malware from a Windows PC

94 Advanced Security Tips

96 Windows 10 Privacy Settings
98 How to Check which Apps are Sending Information
100 What is a firewall?
102 Improving the Windows 10 Firewall
104 Creating a Security Plan
106 Windows Security Checklist
108 What is a Sandbox?
110 Running Windows 10 as a Sandbox
112 Installing VirtualBox
114 Installing Windows 10 in VirtualBox
116 Creating VirtualBox Snapshots of Windows 10
118 Create a Windows 10 Recovery Drive
120 How to Back Up Windows 10
122 How to Create a Windows 10 System Image
124 Extreme Windows 10 Lockdown Tips
126 Cyber and Windows Quiz
128 What the Experts Say



130 Online Child Protection

132 Children Online: What are the Risks?
134 Social Media & Children
136 Search Engine Safety
138 Online Grooming
140 How Safe are the Sites Your Child Can Access?
142 Email and Child Safety
144 Top Child Friendly Email Programs and Services
146 Cyberbullying
148 How to Prevent and Deal with Cyberbullying
150 Helping Your Child Through the Internet
152 Your Child and Online Gaming, is it Safe?
154 Staying Safe when Gaming Online – Advice for Your Child
156 Monitoring What's Going On
158 Monitoring Online Activity for Non-Technical Guardians
160 Tips for Technical Guardians to Monitor a Child's Online Activity
162 Ten Monitoring Tools to Install and Use
164 Using the Windows Hosts File to Block Sites

166 Further Protection for Young Adults

168 Staying Safe with Facebook for Teens
170 Staying Safe with Twitter for Teens
172 Staying Safe with Instagram for Teens
174 Staying Safe with WhatsApp for Teens
176 Staying Safe with Snapchat for Teens
178 Creating a Child Account in Windows 10
180 Windows 10 Family Features
182 Problems with In-app Spending
184 Tips on How to Stop In-app Overspending
186 Online Child Safety at School
188 Where to Find Help with Online Child Safety
190 What the Experts Say
192 Glossary of Terms

Black Dog i-Tech Series
8th Edition - ISSN 2044-4060 Published by: ..Black Dog Media Limited (BDM)
Editor:.. James Gale
Art Director & Production:.......... Mark Ayshford
Production Manager:.....................Karl Linstead
Design:..Robin Drew
Editorial: ....David Hayward
Sub Editor:..Paul Beard

Printed & bound in Great Britain by:
Wyndeham Press Group Limited
Print services supplied by: Media First (International) Ltd
Newsstand distribution by:
Seymour Distribution Limited, 2 East Poultry Avenue
London EC1A 9PT
International distribution by:
Pineapple Media Limited www.pineapple-media.com
Digital distribution by:
Readly AB, Pocketmags, Zinio, Cafeyn, Magzter
For all advertising and promotional opportunities contact:
enquiries@bdmpublications.com

Copyright © 2021 Black Dog Media. All rights reserved.

Editorial and design are the copyright © Papercut Limited and is reproduced under licence to Black Dog Media. No part of this publication may be reproduced in any form, stored in a retrieval system or integrated into any other publication, database or commercial programs without the express written permission of the publisher. Under no circumstances should this publication and its contents be resold, loaned out or used in any form by way of trade without the publisher's written permission. While we pride ourselves on the quality of the information we provide, Black Dog Media Limited reserves the right not to be held responsible for any mistakes or inaccuracies found within the text of this publication. Due to the nature of the software industry, the publisher cannot guarantee that all tutorials will work on every version of Linux Mint, Debian-based or other Linux distributions. It remains the purchaser's sole responsibility to determine the suitability of this book and its content for whatever purpose. Images reproduced on the front and back cover are solely for design purposes and are not representative of content. We advise all potential buyers to check listing prior to purchase for confirmation of actual content. All editorial opinion herein is that of the reviewer as an individual and is not representative of the publisher or any of its affiliates. Therefore the publisher holds no responsibility in regard to editorial opinion and content.

Black Dog i-Tech Series - is an independent publication and as such does not necessarily reflect the views or opinions of the producers contained within. This publication is not endorsed or associated in any way with The Linux Foundation, Canonical Ltd, Debian Project, Lenovo, Dell, Hewlett-Packard, Apple and Samsung or any associate or affiliate company. All copyrights, trademarks and registered trademarks for the respective companies are acknowledged. Relevant graphic imagery reproduced with courtesy of Lenovo, Hewlett- Packard, Dell, Samsung, Linux Mint, Canonical, CyberGhost, BBC News, MINIX, Steam and Valve, Intel, AMD, Crucial, SanDisk, ASRock, CIT, Cooler Master, Nvidia, BenQ and Apple. Windows is a trademark of Microsoft Corporation, registered in the United States and other countries. Windows ©2021 Microsoft Corporation.

Additional images contained within this publication are reproduced under licence from Shutterstock.com.

Prices, international availability, ratings, titles and content are subject to change. All information was correct at time of print. Some content may have been previously published in other volumes or BDM titles. We advise potential buyers to check the suitability of contents prior to purchase.

Black Dog Media Limited (BDM)
Registered in England & Wales No: 5311511

STOP

Information regarding cyber security doesn't always have to be technically heavy. In fact, to make it easier to digest, and to just show you how virulent and bitterly hostile computer-borne security threats are, here's a collection of statistics to give you the heebie-jeebies; all the more reason then to keep this manual close to hand.

80%	of all cyber crime attacks originate from Russia, China and North Korea
77%	of small businesses **don't** regularly back up important data
75%	of the health care industry has been infected with malware.*
73%	of US citizens have fallen victim to some form of cyber crime
64%	of companies have experienced web-based attacks
61%	of malicious websites are genuine sites that have been compromised

Over the next year there is a

69%

CHANCE

you could be

HACKED!

Social Media Users

50%

*****_

Haven't changed their password in the ***last year***

20%

*****_

Have ***never*** changed their password

Sources: Symantec Corporation Threat Report ◆ CSO Cybersecurity Business Report ◆ UK National Cyber Security Centre ◆ Security Intelligence ◆ Hackmageddon.com ◆ UK Office for National Statistics ◆ Bitdefender Labs Report ◆ Herjavec Group

* Figures based on 2017 half yearly report.

A member of the public is **HACKED** every:

39 SECONDS

Devices hacked in **LESS THAN:**

2 MINUTES

RANSOMWARE ATTACKS on BUSINESS every:

40 SECONDS

250,000 NEW VIRUS threats **EVERY DAY**

GLOBALLY: COST PER PERSON **6 MONTHS***

$123

FIXING Malware ATTACKS

$441

LOST to **Cyber CRIME**

$271

PAYING RANSOMS to remove malware

OVER 3,000,000

REPORTED INSTANCES OF **FRAUD**

through **cybercrime** against **UK banks** last year

Statista.com • iQuda.co.uk • Tektonika • Securityaffairs.com • Ic3.gov • Marblesecurity.com • Infosec Institute • IBM • The Linux Foundation • Microsoft • ITworld.com • Javelin Strategy • US Government • NSA.gov • CIA.gov • Whitehouse.gov

Modern Day Security

The start of the digital age brought with it many advances in the way we work and interact with each other. It's estimated there's 1.2 Zettabytes (1.3 trillion gigabytes) of data available to someone with access to the Internet and whilst most of it may be irrelevant, what's important to you is somewhere within that mass of raw information.

Sadly, the cold hard light of day reveals that with the growth of this voluminous data comes the nefarious acts of those who wish to cause mayhem, panic, theft and other such negative elements. Therefore, as a user you need to make sure that you're protected against the ever increasing digital world of threats, viruses and everything else the Internet has to offer.

This chapter will help you to recognise some of the threats, what they all mean and how they work. We can help you to identify and know what to look out for when online.

10 Types of Security Risk
12 Hackers and You
14 Social Engineering
16 Ransomware: How it Works
18 The Virus Top Ten
20 Phishing, Vishing and Smishing
22 Pharming
24 Windows 10 Security
26 Digital Security FAQ

Types of Security Risk

There are more security risks for your computer than just the common, run-of-the-mill virus. The amount of digital use the average person has over the course of a week has increased significantly in just a few years, and with it comes a legion of security related issues.

Here Be Dragons

This isn't a definitive list of the possible threats available for the Windows user but here are ten modern risks that you face every time you power up your PC.

01

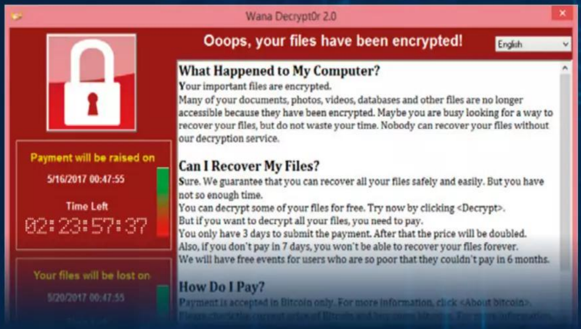
Viruses

Viruses have been around for as long as computers. They've moved on from simply displaying the name of the coder on the monitor, a kind of virtual vandalism, and now can disable and wipe the data off a hard drive in mere seconds.

02

Ransomware

Earlier in the year the UK was gripped in the clutches of the WannaCry ransomware infection. This particular infection exploited a vulnerability in Windows, and quickly spread throughout the NHS and other organisations, locking and encrypting the data on a computer until money was sent to those who unleashed it to the world.



What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Payment will be raised on: 5/16/2017 00:47:55

Time Left: 02:23:57:37

Your files will be lost on: 5/20/2017 00:47:55

03

Worms

Although a worm is a type of virus, it behaves differently in that it's goal isn't to alter or destroy system files. Rather, it's designed to replicate itself continuously until all the resources and space on the system are consumed. A bit of a nightmare for the system administrator.

04

Trojans

The Trojan horse, as the name suggests, is a program that masquerades as a legitimate application but in actual fact contains code that allows a hacker remote access to your computer. Like the legend of the wooden horse the Greeks used to gain access to Troy, once inside your computer it opens and creates an opening for the hacker.

05

Spyware

Spyware invades computers usually through freeware or shareware downloads, which is why you should always download a program from a reputable source. The intent of spyware is to collect information about the user and report it back to those who wrote it.

06

Adware

Adware is very similar to spyware, in that one of its goals is to monitor the user. However, adware usually goes one step further and bombards the user with Internet pop-up advertising, usually when they open their browser or a new tab. The advertising can be tame, such as gardening equipment, or it can be extremely offensive.

07

Hacking

While Hollywood would have you visualise the lifestyle of a hacker as something that's quite alluring, in truth it's quite the opposite. The average user is generally under the radar where a hacker is concerned. They're mostly after the corporations, or famous people, but you can have your computer hacked by a neighbour, for example.

08

Social Engineering

A relatively modern term in the history of computer security, social engineering will have the user deceived into giving away personal information or allowing a scammer into their systems. The recent spate of calls from people claiming to be from the likes of Microsoft or a security firm are a prime example.

09

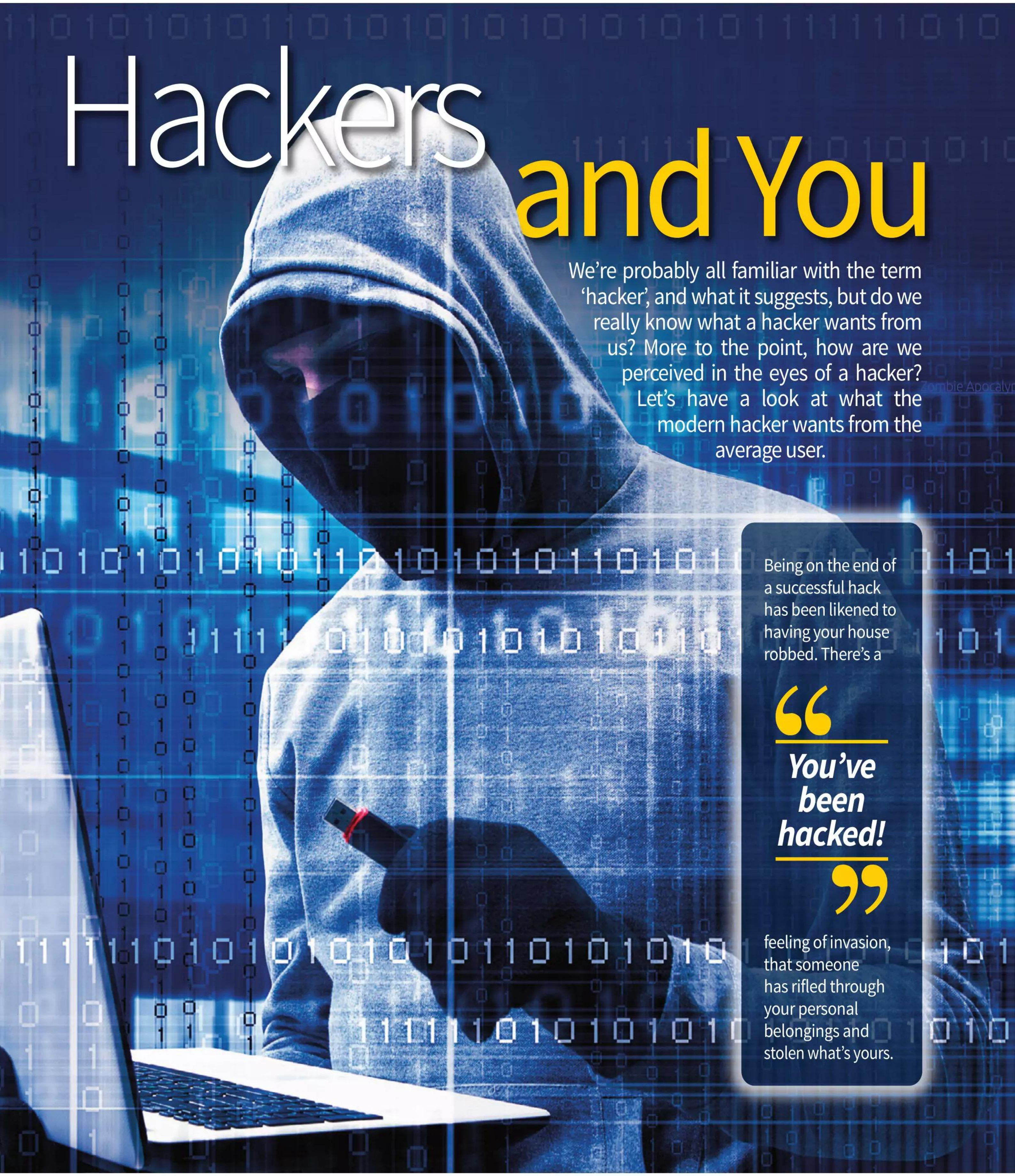
Phishing

Much in the same vein as social engineering, phishing is the act of obtaining sensitive information (bank details usually) about a user by being disguised as a trustworthy source. Phishing on social media sites such as Facebook, Twitter, etc. is on the rise.

10

Rootkits

Rootkits are virus-like programs that are activated before the computer's anti-virus and security suites are started when booting Windows. They can change the way a security suite looks at files, allowing a virus to hide in plain sight and not be detected by the system's security measures.



Hackers and You

We're probably all familiar with the term 'hacker', and what it suggests, but do we really know what a hacker wants from us? More to the point, how are we perceived in the eyes of a hacker? Let's have a look at what the modern hacker wants from the average user.

Being on the end of a successful hack has been likened to having your house robbed. There's a feeling of invasion, that someone has rifled through your personal belongings and stolen what's yours.

> “*You've been hacked!*”

WARNING

Monetary Motivation

As with most hacks the world over, money is the driving force behind an attack. A hacker will want to enter your system through various means and obtain your bank or credit card details in order to get access to your money. It's plain and simple theft.

Personal Information

Personal information can be extremely valuable to a hacker. Those who manage to obtain information about you, from date of birth, address, social security number and countless other trivial details, can then use your identity to open bank accounts, start a loan and so on. In the end, it is your name that's linked to the fraud.

Parasitic Infection

Sometimes a hacker will use you to get some other target. Perhaps you work at a bank, or something similar, the hacker will then identify you as a target that can be used to transfer a program from your laptop to the work's server. You unwittingly become the carrier of malware, allowing a hacker to gain access to your work.

Exploitation

Exploitation is becoming a common theme among modern hackers. In this scenario a hacker will gain access to your personal information and hold it to ransom. They can then demand anything from money, to more personal acts.

Stealing Bandwidth

Rather than targeting a user purely for financial gain, or something else, a hacker can also want to use your home bandwidth. Generally speaking, the hacker doesn't need to be on the other side of the world, they could be a neighbour who's using your Internet connection to download copyright material.

Access to Your Webcam

Webcam hacking has become more popular in recent years. What happens here is, a hacker manages to gain access to your computer and activates the webcam in order to view what you're doing; and as long as the computer is up and running, they can see everything the webcam can, and they can do so without you even knowing.

Access to Your Microphone

To expand on the previous hack, along with a webcam hack an attacker can also activate a computer or device's microphone. Doing so will allow them to listen in on anything that's being said, so perhaps it's worth covering up your microphone during any future meetings.

Zombie Apocalypse

There are instances whereby you become the target of a larger scale hack. In this case the hacker isn't targeting you specifically, they're simply using your computer as a zombie, a collection of machines connected to the Internet that runs malicious programs against a target. Zombies are often used to conduct DDoS attacks.

Cyber Vandalism

Often you can be the target of an attack that doesn't seem to make any sense. The hacker doesn't want money, they don't want your personal information either. It's just a case of cyber vandalism. Perhaps the hacker wants their name known in the wider world, or just likes to see chaos reign. Who knows why they do it?

Distributing Illegal Material

Finally, a hacker can use your computer as a source or a node for the distribution of illegal material. You won't even be aware of the fact but your computer is successfully trafficking illegal material together with others on the Internet.

Social Engineering

With the rise of wider forms of communication, through social media and so on, comes a new wave of threats called social engineering. There are many forms of social engineering, so let's have a look at what you're up against, and how to combat it.

Social engineering is the new modern way of manipulating people to give up their personal and confidential information. It comes in many guises and under different sub-headings, such as Phishing and the like, but it's essentially all a form of social engineering. Essentially, the scammer will take your human nature and responses and turn it against you for their own gain.

The kind of information the scammer is after does vary, depending on the type of scam being used, but for the most part they're usually after your passwords, bank and credit card details, or login information in order to gain any sort of financial data.

You're probably more familiar with social engineering that you suspect, even if you're new to the term. Recall the emails from someone, usually based in Nigeria, who has come into a fortune in the billions and for some inexplicable reason wants to put the money in your bank account. Needless to say, the money was never there in the first place and should you go through the process you will eventually be persuaded to hand over some banking information which the scammer can then use to steal from you.

There aren't too many Nigerian scams these days, mostly you get a phone call from someone claiming to be from Microsoft or some other well-known company, who insists that they are tracking a virus or other harmful malware that's currently residing on your computer. They ask you to visit a webpage and download a piece of software that will allow them remote access to your computer. When in, they run a script that displays a wealth of useless information on the screen whilst in the background they run keylogging and hacking software to obtain your online banking details. They can even ask you to log into your bank while connected to make sure everything is working.

Other common social engineering tactics include emails from a friend, who has been hacked, with the scammer masquerading as them. It could be an email claiming to be from your bank, an urgent request for help or someone asking for a donation to a charitable organisation. Be wary, and question everything.

You may think you're not the sort of person to be fooled by a scam but often the

> **“Scam, scam, and more scam”**

scammers have employed subtle ways and means in which to bait you.

Foreign offers are fake

If you've received an email or a pop-up on a website offering you some financial reward, then it's more than likely to be fake. Likewise, lottery funds from other countries are fake too, as is money from so called Uncle Charlie who lives in Outer Mongolia.

Slow down

Many scammers want you to react quickly, as a matter of urgency. Take a moment to figure out what's going on and don't fall for any high-pressure tactics. Ask for half an hour to call a friend for advice.

Research everything

Locate your bank or credit card company's webpage and follow any links to known social engineering scams. Read all the information you can gather about the techniques and tricks used and arm yourself with that knowledge prior to any contact from a scammer. The more you know, the less likely you are to being hoodwinked.

Don't engage

Whilst it's fun to lead a scammer on the other end of the telephone, telling them that the only computer you own is a Commodore 64, it's really not worth it. They know they're scamming, you know they're scamming, so just put the phone down and ignore them.

Never give your password

A bank never asks you for your password, they never call you up or send a text message requesting to enter your password, nor will they ask you for other personal information relating to your account. Treat all requests as suspect and don't give out any of your passwords.

Beware of attachments

Email attachments are an excellent way of distributing malware, viruses and hacking scripts to your computer. If you receive an email claiming to be offering you a deal of a lifetime, and requesting you open the attached file, then it's likely a virus. Research the sender, and best to delete the email.

Ransomware: How it Works

The first instance of an extortion attack is credited to Joseph Popp back in 1989. Since then the frequency, delivery and scale of ransomware attacks has increased significantly; so what is ransomware and how does it work?

Ransomware is a particularly nasty form of malware and digital threat. There's usually some kind of ransomware headlining in the news around the world and those who are the victims are often at a loss as to what to do next.

Essentially, ransomware will infect an individual computer and one of two things can happen: first, it locks the computer, stopping all access to it from the keyboard, then it starts to search for data and encrypt the contents of the hard drive. Lastly it infects the boot sector of the computer and displays a message detailing the type of ransomware and how the individual will pay for the release of the data; the message can even have fake FBI warnings included with it. Alternatively, and the second thing that may happen once a system is infected, the ransomware will lay in wait until a set time and date, then do all of the above and lock the computer. Waiting for a set time will ensure that numerous machines are infected before any fix can be discovered; also if all the infected machines are activated at the same time then there's more of a chance of the attacker getting their ransom paid.

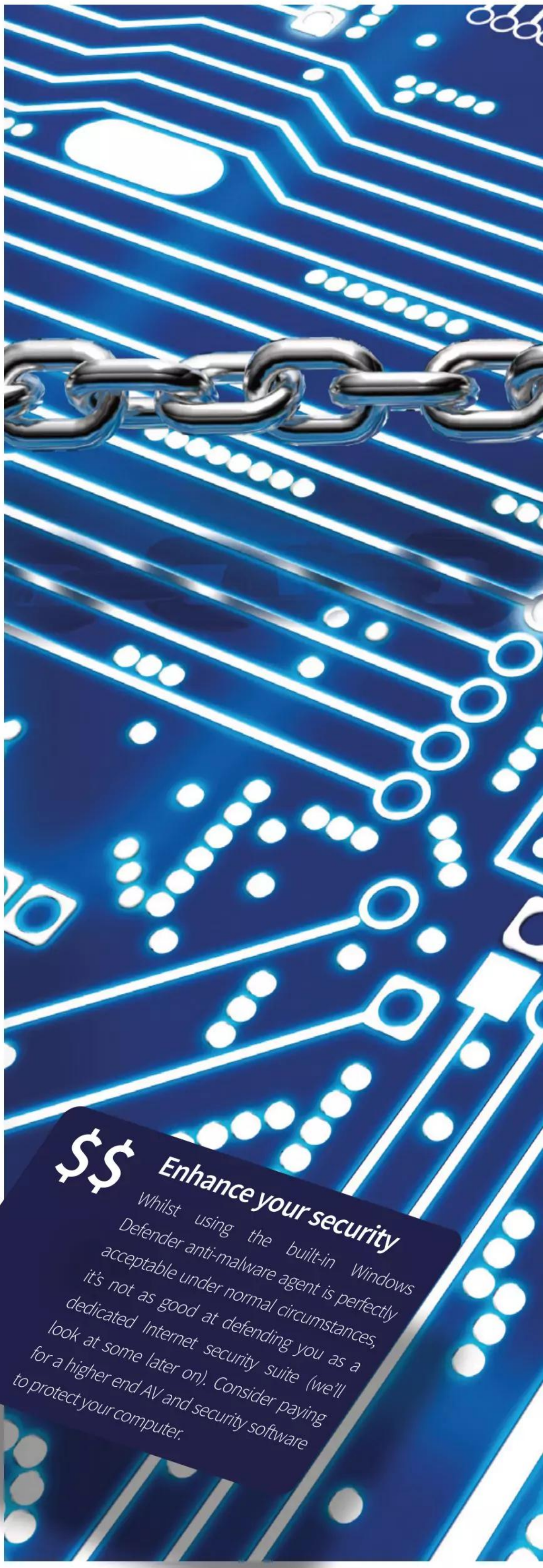
You normally have a set time in which to pay the ransom, usually 72-hours. If the victim doesn't pay in time, the attacker can introduce a second phase into the ransomware code that will either increase the amount demanded or completely destroy the files that are being held at ransom.

Ransomware can be spread in a number of ways. The more popular choice of delivery is via an infected web page, some form of Flash script that has been hijacked and now contains a link to a remote server where the browser will unwittingly download the ransomware code. More recently there are instances of Drive-by attacks, where the ransomware code locates any USB sticks a user may have in their system and transfer itself in the knowledge that the stick will be inserted into a work's computer.

The WannaCry ransomware attack earlier in the year was by far one of the most prevalent in recent years. It's estimated that more than 250,000 computers across 200 countries were infected, rendering the likes of big companies such as FedEx, Nissan Motor Co and Telefonica SA under siege from its demands. The National Health Service in the UK was hit too, resulting in weeks of chaos and disorder for the staff and patients alike.

“What to do”

How do you avoid getting ransomware on your computer and what happens if you're unlucky enough to be the target of such an attack? Here are some hints and tips for you.



$$ Enhance your security

Whilst using the built-in Windows Defender anti-malware agent is perfectly acceptable under normal circumstances, it's not as good at defending you as a dedicated Internet security suite (we'll look at some later on). Consider paying for a higher end AV and security software to protect your computer.

$$ Updates

The single most important factor of preventing a ransomware attack is to make sure that your computer has the latest updates applied. Ransomware code usually looks for vulnerabilities and weaknesses in the operating system but if they're up to date and patched, then it's difficult for it to activate.

$$ Never insert a random USB stick

If you've found a USB stick somewhere, although the temptation is strong to see what's on it, don't stick in your computer. Not only could it be infected with all sorts of malware, it could also contain sensitive and confidential data. Either destroy it or hand it over to a security expert at work.

$$ Never pay

Your data is locked, and there's nothing that can be done by anyone to save it, so it's really not recommended to pay the ransom. Nine times out of ten, the attacker will take the money and never unlock the data anyway. There's also the threat of more malware being activated after payment.

$$ Backup

Set yourself a daily backup schedule, to a USB, cloud or network resource that's separate from your computer. If your data is securely backed up, and you get a ransomware attack, then you can happily wipe your computer, re-install Windows again, then copy the saved data back over.

The Virus Top Ten

Viruses are constantly evolving thanks to more ingenious methods of delivery and due to the developers and hackers tweaking their code to sniff out operating system vulnerabilities. It's difficult to say what the next big virus will be but some scary ones have already appeared on the Internet.

Just to give you an idea of what the future could hold for the computing world,

> **“*Digital Destruction*”**

here are the top ten most destructive viruses unleashed over the last decade into the digital domain.

1 Storm Worm

Storm Worm was released in 2007 and was rumoured to have hailed from Russia. It came in the form of an email link, usually with an important headline to grab the victim's attention. When the victim clicks the link the code is inserted and payload with a backdoor into the system is opened. It infected over 10 million computers worldwide.

2 Conficker

Conficker was a 2008 worm that infected an estimated 15 million Windows computers worldwide. The French Navy, UK Ministry of Defence, hospitals and local police forces were affected. It was spread via Facebook, Skype and mail services, and infected networked computers with a keylogger that the hacker could use to record your keyboard strokes.

3 Daprosy Worm

2009 saw the release of the Daprosy Worm whereby an estimated 20 million computers were infected with a keylogger. What made this such a dangerous virus was that it remained active in Windows Safe Mode, so it was very difficult to remove.

4 Stuxnet

Stuxnet was rumoured to have been a US Intelligence created virus that was designed to infect Iranian nuclear power plants, thus stopping them from potentially creating weapons grade material. Whether you believe that or not, it was one of the worst viruses to appear in modern times.

5 Duqu

Duqu was released in 2011 and shared many characteristics with Stuxnet. However, Duqu had different roles: it would work as a keylogger, to steal digital certificates, gather information about an infected PC, or completely wipe the contents of any connected hard drives. Interestingly, parts of the Duqu code were written in an unknown high level programming language.

6 Shamoon

Shamoon was discovered in 2012 and developed to infect the Windows kernel, the core code of the operating system. It successfully managed to wipe the contents of millions of hard drives and was rumoured to be used in cyber espionage in the energy industry.

7 CryptoLocker

CryptoLocker is a ransomware infection that first appeared in 2013. As with most ransomware code it locks and encrypts your entire hard drive and offers to unlock them if the victim pays up to $300. Remarkably, the code was able to delete itself whilst still keeping the files encrypted and locked.

8 Regin

2014's Regin virus was spread via fake websites and infected tens of millions of computers. Rumour has it that it was a joint US and UK intelligence created virus for global digital surveillance but we'll leave that for the conspiracy theorists to argue over. Nevertheless, it managed to send information of the victim's computer back to an unknown location.

9 Rombertik's Endless Loop

Rombertik's Endless Loop is an interesting, if somewhat deadly, virus to have sprung up in 2015. When infected, the virus will alter and delete key boot files for Windows computers then force them to reboot. With the boot files missing or altered the Windows PC will continually boot and reboot itself until you re-install the OS.

10 Tiny Banker

Tiny Banker is an information and packet sniffer virus that will record any online banking details the victim enters in their computer. That information is then sent back to several servers which the hackers can then use to access your bank accounts. It's estimated that hundreds of millions were stolen in 2016 thanks to Tiny Banker.

Phishing,

It's tempting to think we've made up the words Phishing, Vishing and Smishing but in actual fact they're all forms of social engineering scams. Whilst we've covered social engineering already, it's worth looking at these three modern day threats individually.

Social engineering, the act of getting information from a person based on their human instinct to react, help or be entrapped into some form of false promise, isn't as modern as the name suggests. Although the term 'social engineering' is in fact relatively new, the process of obtaining sensitive information from a victim has been around for a very long time.

The digital age, of course, has increased the attacks and how they're delivered. No longer is a victim beguiled by post, now they're bombarded by false websites, emails and a string of other cleverly disguised mediums.

Let's break down the three main, modern methods of how a scammer will attempt to obtain your personal and sensitive information: Phishing, Vishing and Smishing.

Social engineering fraud comes in many guises, with oddly sounding names and methods. In the end, the scammers are after your data, but what do these three in particular mean?

> *Gone Phishing*

Phishing is the attempt to obtain information from a potential victim through emails, messaging, social media and auction sites. They can come in the form of an email, for example, claiming to have some money available for you or pretending to be from your bank or credit card company. Social media phishing includes individuals befriending you, or pretending to be someone you may know, then asking for information. Similarly a phishing attack can come in the form of a Facebook seemingly friendly test, such as 'name the top five things about yourself and tag ten friends…'. The unwitting victim will happily reveal their date of birth, where they were born, pets names, names of any children and so on. The attackers will gather all that information and use it to their advantage.

Interestingly there are also three different phishing types: Spear, Clone and Whaling. Spear phishing is designed to specifically target an individual, gathering information such as the above Facebook 'game' whereby the scammer can personalise their attack on the victim.

Clone phishing is an attack type that uses a previously delivered, legitimate email containing an attachment but with the details changed and the attachment swapped for a virus or keylogger. To the victim the email looks real, since it's cloned from a real email, and when the attachment is opened it infects the computer.

Whaling is when a phishing attack targets senior executives of a company or a high-profile individual or business. The attack is a finely crafted email or web address that's created to look business-like and containing information specific to the company or individual. ■

Vishing & Smishing

Vishing is voice phishing, using a telephone call to commit some form of social engineering attack. The victim will, as we've explained previously, receive a call from a legitimate sounding call centre with the person on the line claiming to be from a well-known computer related company. Usually the caller will be led to believe that there's a virus on their computer or that some form of security vulnerability has been detected. The victim will then be guided to a website where the caller can make a remote connection to their computer. Once on the victim's computer, the caller will then run a script that will display reams of data on the screen designed to confuse and baffle the victim. In the meantime, they're secretly running a keylogger in the background.

In some circumstances they can then claim to have fixed the so called issue but ask you to log into your bank to double-check all is well. With a keylogger in place, they can then see your username and password on their screen; after which they log in and steal from your account.

Alternatively an automated call can ask you to enter your credit card number into the phone's keypad, as it's been reported as being used elsewhere. Of course it hasn't but as soon as you enter the details they're recorded and your card can be used by the scammers. ■

Smishing is an SMS form of phishing. In these cases you receive a text from a seemingly legitimate source, usually your bank or credit card company but also in the form of a competition winner or something free, asking you to confirm your details. There's often a link for you to follow, which leads to a false website that logs your keystrokes and records your data.

Some smishing attacks will ask you to send a return SMS to approve an action, such as a delivery of some goods. The return message is designed to cost significantly more than the usual SMS rate, with the money going straight to the scammers.

One way or another, each of these scams are designed to bait the victim, hence the phishing element, a homophone of the word fishing. The best defence is to ignore, delete or hang up on anything that's even remotely suspicious. Microsoft doesn't know if you have a virus, and nor will it telephone you. Your bank won't email you for your account details and don't be tempted to fill in any Facebook games with personal information. In short, be savvy about baiting techniques and remain vigilant. ■

Statistics
Progress
Growth & Decline
ANNUAL PLANS

Pharming

Whilst on the subject of homophones, another recently added word to the long list of security threats is Pharming. Pharming falls within the online fraud layer of security and although in reality it's been around for as long as web pages have, the methods of deception are continually evolving.

So what exactly is pharming? In short, this is the criminal act of producing a fake website and redirecting the victims to it. The website could be anything from a reasonably popular online shopping store, to one of the well-known high street banks. The victim, unaware that the web site is fake, as the front end apes the real thing, even down to the small print at the bottom of the page, will login with their details.

After the user has logged in several options are available to the 'pharmer'. They can collect the username and login details and simply leave the victim with a blank web page; this is usually a method used by an amateur pharmer or those who want a quick username and password grab before disappearing into the darkened corners of the Internet. Otherwise, they can redirect the victim to the real site where they need to enter their login details again. The latter is a more convincing method of pharming, as the victim rarely questions why the bank has asked for their login credentials twice; they often put this down to a mistaken entry on their part.

Either way, the pharmer now has a considerable list of valid usernames and passwords for the bank or online shop they faked, which they can then sell via the Dark Web or use themselves. How do they, the pharmers, get away with being able to do this? Interestingly, there are several ways in which someone can fake a legitimate website.

Pharming has become quite sophisticated in recent years, and with the rise of connected devices that offer Internet access it's quickly become one of the more popular criminal cyber activities.

> “*Harvesting Time*”

http:// DNS

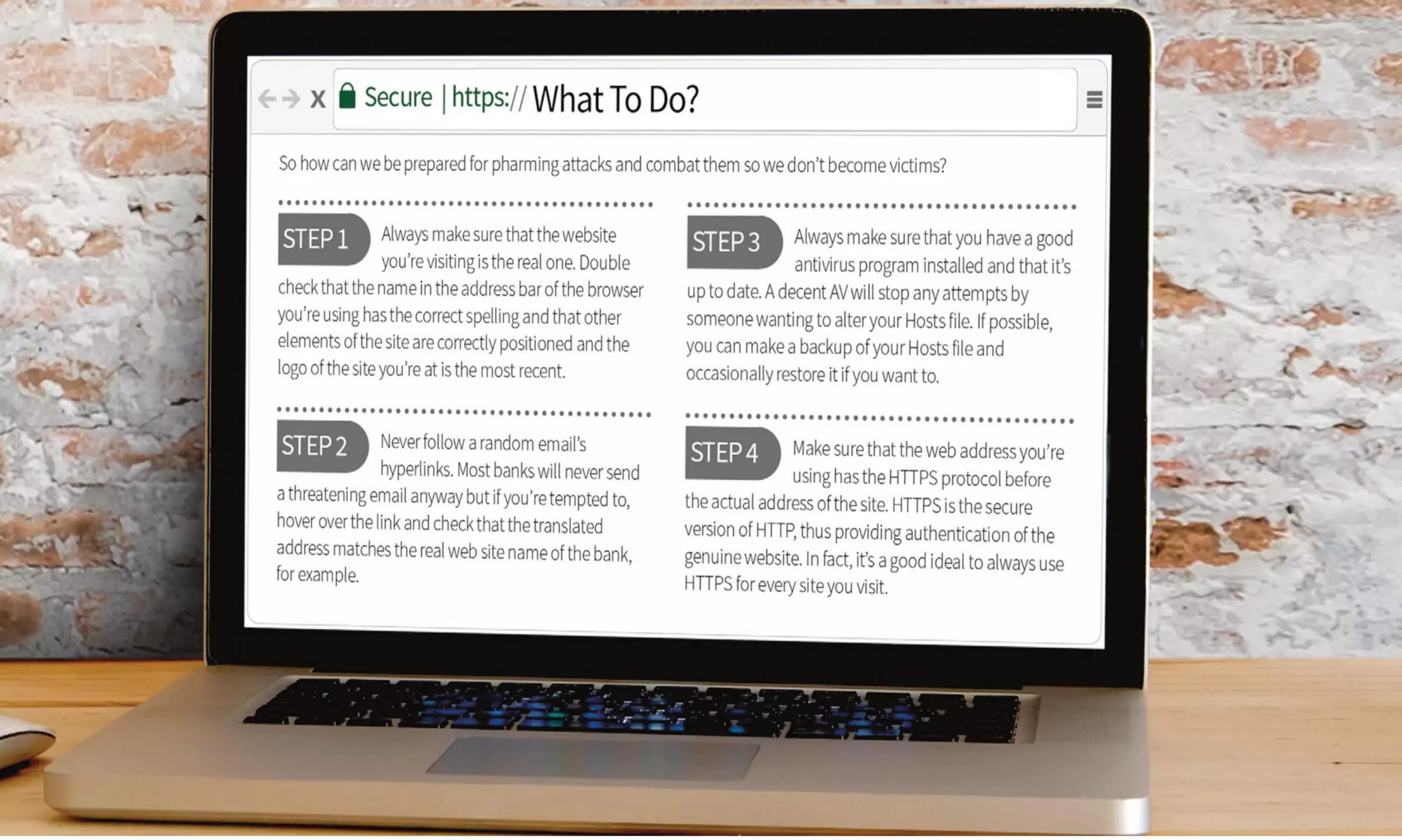
DNS cache poisoning is the primary method of creating a fake website with the view to setup a pharming scam. This involves the criminal attacking the Internet naming system, which is responsible for creating readable names for websites, such as www.ebay.com and so on, rather than a string of numbers in the form of the IP address, such as www.184.232.124.65 or similar. The Internet naming system relies on DNS servers to provide the conversion between IP addresses and readable web site names. The attacker can mount an attack on the DNS cache, thus changing the way in which traffic moves on the Internet. Effectively, instead of the user's request to go to www.ebay.com, they're taken to the attacker's fake website instead. Thankfully, these kind of attacks generally don't last for long, as the DNS cache is monitored frequently by many different engineers and companies.

http:// Fake Naming

Fake naming relies on the attacker seconding their pharming attempts with a phishing email. The email can look legitimate and contain relevant information about the person in general. There's often a link at the bottom that although is spelt correctly in the email, is in actual fact a hyperlink to a pharming website that's similar to the real thing but spelt somewhat differently. For example, the email could say 'your overdraft is nearing its limit, please login to www.bank.com to transfer funds…' The www.bank.com part is correct, but the hyperlink and the resulting website may be taking you to www.bnak.com, which although subtly misspelt is often difficult to miss when you're concentrating on the website content.

http:// Hosts

One method that's more difficult to pull off, though if successful is remarkably effective, is to alter the victim's Hosts file on their computer. The Hosts file is located in C:\Windows\System32\drivers\etc\hosts on Windows computers, /private/etc/hosts on macOS, and /etc/hosts on Linux computers. Its function is to map hostnames to IP addresses, translating the readable websites to IP addresses on a local network. However, it can also be used to circumvent the Internet lookup of a legitimate web site, redirecting you to a fake one. It's not often that the Hosts file can be altered, as it's a system file that requires elevated permission in order to edit, but a cleverly written virus can do the trick.



Secure | https:// What To Do?

So how can we be prepared for pharming attacks and combat them so we don't become victims?

STEP 1 Always make sure that the website you're visiting is the real one. Double check that the name in the address bar of the browser you're using has the correct spelling and that other elements of the site are correctly positioned and the logo of the site you're at is the most recent.

STEP 2 Never follow a random email's hyperlinks. Most banks will never send a threatening email anyway but if you're tempted to, hover over the link and check that the translated address matches the real web site name of the bank, for example.

STEP 3 Always make sure that you have a good antivirus program installed and that it's up to date. A decent AV will stop any attempts by someone wanting to alter your Hosts file. If possible, you can make a backup of your Hosts file and occasionally restore it if you want to.

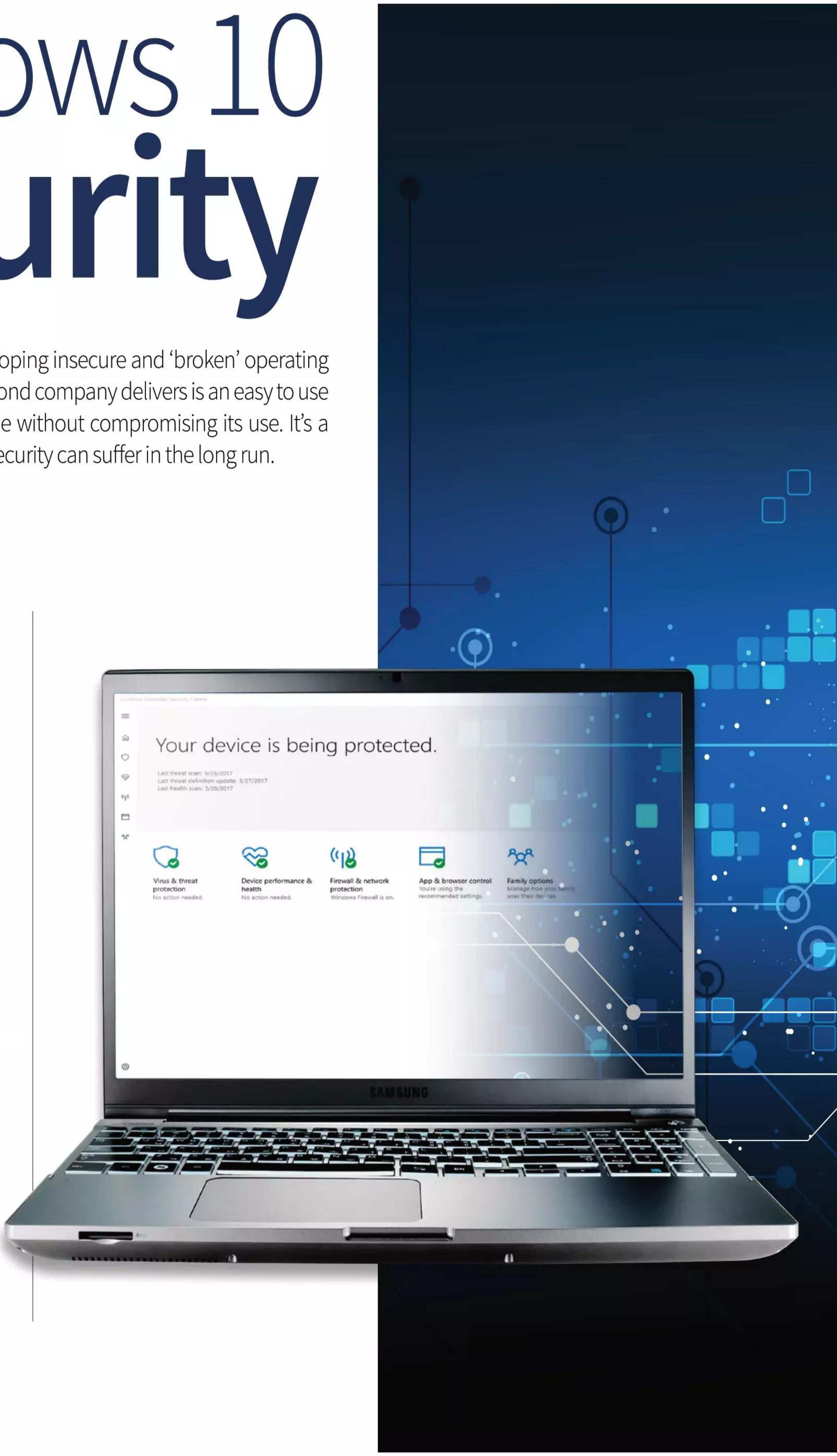
STEP 4 Make sure that the web address you're using has the HTTPS protocol before the actual address of the site. HTTPS is the secure version of HTTP, thus providing authentication of the genuine website. In fact, it's a good ideal to always use HTTPS for every site you visit.

Windows 10 Security

Microsoft is often accused of developing insecure and 'broken' operating systems. However, what the Redmond company delivers is an easy to use system that's as secure as it can be without compromising its use. It's a difficult balance to maintain and security can suffer in the long run.

Security leaks, holes and flaws in development code appear all the time, for every operating system. Windows 10 has the bad luck of being at the top of the security flaw news pile. However, here are ten reasons why it's actually a secure OS to use.

> **"Windows 10 Security Improvements"**


Windows Defender Security Centre

Your device is being protected.

Last threat scan: 5/23/2017
Last threat definition update: 5/27/2017
Last health scan: 5/28/2017

Virus & threat protection
No action needed.
Device performance & health
No action needed.
Firewall & network protection
Windows Firewall is on.
App & browser control
You're using the recommended settings.
Family options
Manage how your family uses their devices.
SAMSUNG

Virtualisation-based Security

VBS is an improvement to the core Windows security, it stands for Virtualisation-based Security and uses a mixture of hardware and software enforced developments to create an isolated, hypervisor restricted subsystem for securing the OS core data. Nothing unsigned by Microsoft is allowed to be injected into the kernel or executed.

Secure Booting

Secure Booting utilises the new UEFI (Unified Extensible Firmware Interface), the replacement for the older and more vulnerable BIOS, along with Windows Trusted Boot code integrity and ELAM (Early Launch Anti-Malware) capabilities, to protect the computer as soon as you power it up.

Windows Hello

Windows Hello may seem like a glamorous feature rather than a security feature but it's really quite an impressive layer of protection. Hello supports passwordless biometric authentication methods, such as iris, facial and fingerprint, together with a PIN code to help protect access to Windows 10.

Microsoft Passport

Windows 10 uses the Microsoft Passport single sign on solution that supports the open FIDO Alliance security authentication standard (www.fidoalliance.org) and utilises cryptographic keys to secure access to network and local resources.

Trusted Platform Module

If your computer has a TPM chip (Trusted Platform Module), Windows 10 can utilise the hardware cryptographic key therein to link Passport and Windows Hello to authenticate the user and operating system with local, network and Internet resources.

Credential Guard

Windows 10 Credential Guard protects the user details and Windows authentication keys within the VBS layer. This isolates the authentication service against network and local attacks, stopping keyloggers and other worms from gaining your login details.

Device Guard

Windows 10 has introduced Device Guard, a highly secure tool that determines which programs and scripts should be allowed to run on the computer. It utilises the VBS layer to protect the core system files and with a list of what's allowed and not allowed to run it can prevent most malicious content from being executed on your system.

Rolling Upgrade

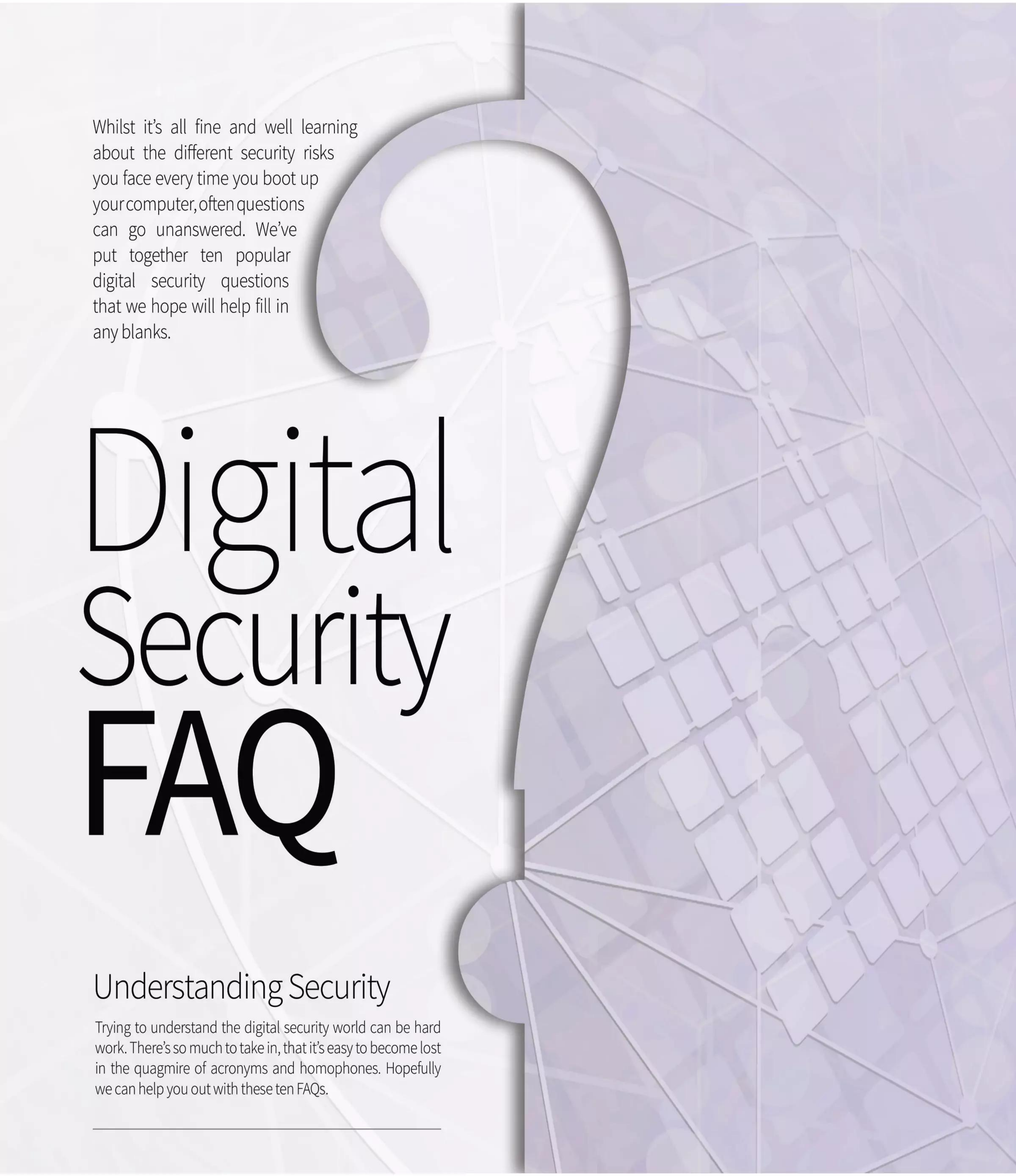
Windows 10's unique method of upgrades now ensures that the latest versions to software, tools and applications are continually upgraded on the computer. The new rolling upgrade process has been widely criticised by many, as there's no opt-out for upgrades available. On the flip side, you're always up to date.

Windows Defender Security Centre

Windows Defender Security Centre is significantly improved over previous versions of the software. The new Fall Creators Edition version offers virus, ransomware and threat protection, device health, firewall protection, app and browser control and family options all under the one roof.

Protection Features

Among the aforementioned security elements, Windows 10 offers User Account Control, Kerberos Armouring, Smartscreen, TPM Key Attestation, Advanced Auditing Settings, Mandatory Integrity Controls, Virtual Smartcards, EMET enabled protection and many more impressive protection features.



Whilst it's all fine and well learning about the different security risks you face every time you boot up your computer, often questions can go unanswered. We've put together ten popular digital security questions that we hope will help fill in any blanks.

Digital Security FAQ

Understanding Security

Trying to understand the digital security world can be hard work. There's so much to take in, that it's easy to become lost in the quagmire of acronyms and homophones. Hopefully we can help you out with these ten FAQs.

Do I need an antivirus program?

Without a doubt, yes. Windows 10 uses the built-in Windows Defender program to help protect you online. It's more than ample for most users but often better security is required.

Viruses and malware are only on dodgy sites, right?

No, sorry. Even legitimate websites can be infected with a virus or some other form of malware. Remember too, a computer virus can enter your system in other ways, not just online.

Is online banking safe?

Online banking is remarkably safe and utilises the latest and continually evolving security encryption methodologies. There's military grade security at every level of the online process, and it's highly unlikely to be hacked.

Are hackers after me?

Whilst it's true that most hackers aren't interested in the average user, they're after bigger targets, there are instances where you could be targeted for one reason or another. Generally speaking, the average user will only be targeted en masse in a country-wide phishing or similar attack.

Can I keep a phishing phone scammer on the line?

Yes, there's nothing stopping you. A school of thought is that while you keep them on the line, turning it into a mock-prank call, you're saving someone else from being duped. However, it's best to simply tell them you know they're trying to scam you and hang up.

Does having extra security cost?

Most of the security changes you can adopt don't cost anything, just you being more aware and knowledgeable about what's going on. In terms of an antivirus product, most of the better total security suites will cost you an annual subscription.

How often do I need to update everything?

Windows 10 keeps a continual update cycle in operation, delivering the latest updates in the background. However, it's always best to do a daily check for any updates for both Windows and any programs you regularly use.

How do I know if something being offered is a scam?

That's a difficult question to answer. More often than not, if it's too good to be true then it's likely to be a scam of some form or another. There are times though when genuine offers are made. It's best to research as much as possible before committing to anything.

I think I've just been scammed, what do I do?

If you think you've been scammed, you need to quickly make some changes: change your Windows password, inform your bank that your details may be compromised, email friends and relatives that you've been scammed, file a police report, scan your computer for threats and check your credit card reports.

I've opened a scam email attachment, what do I do now?

There's a good chance you may have a virus on your computer. Close all open programs, open Windows Defender and do a Full Scan of the system. If anything is detected Defender will tell you what to do. Then, consider a third-party AV suite and scan the computer again.

VPN
Disconnecting...

Protecting Yourself

Being able to recognise a scam or virus is one thing but you need to know how to protect yourself against possible attacks. We look at the top Internet security packages, from Bitdefender, Kaspersky and McAfee, as well as what encryption is and how to make it work for you.

Using a Virtual Private Network is an excellent way to improve your Windows security, we'll look at how a VPN works, what the best VPNs are and how to install and use one on your PC.

30 Be Smart
32 Top Ten Antivirus and Security Packages
34 Bitdefender Total Security 2018 Review
36 Kaspersky Total Security 2018 Review
38 McAfee Total Protection Review
40 Setting Up Windows 10 Security
42 Why Updating is Important
44 What to Keep Updated and How
46 How to Secure Your Web Browser
48 How to Secure Your Home Network
50 What are Wireless Security Standards?
52 How to Secure Your Wireless Network
54 What is Encryption?
56 Encrypting Your Windows 10 Laptop
58 Top Ten Encryption Tools for Windows 10
60 What is a VPN?
62 How Can a VPN Improve Windows Security?
64 Top Ten VPNs
66 Using a VPN for Added Security and Privacy

Be Smart

We've looked at some of the many varied ways in which you can be compromised by a digital attacker and some of the ways in which you can help protect yourself. However, it's often more beneficial to be able to recognise the signs of a digital security issue.

Weakest Links

In terms of digital security, you're only as strong as the weakest link in your security chain. You can tick all the security boxes but if you don't know what to look for in the first place you're still vulnerable.

PASSWORD CHANGE

A good sign of a breach in your digital security is the sudden changing of a password. It can be for a random site, webmail or just something small to begin with. Sometimes a hacker with a keylogger in place will test the water before accessing your bank, in which case you need to virus scan your PC immediately.

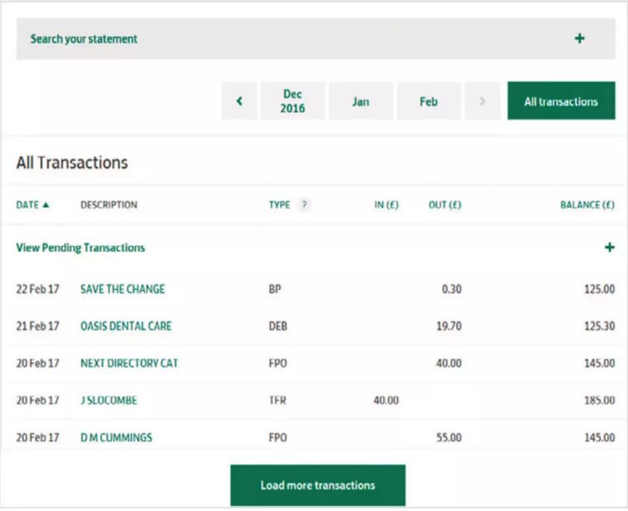
PERSONAL SPAM

We all receive spam emails of some form or another. However, if you suddenly start getting emails of a more personal nature, then you need to look at where that information could be coming from. The details could be your full name, date of birth, knowledge of any children or even a recent accident you may have been involved with.

Sent Mail
Spam (372)
Trash

BANK ACTIVITY

If you check your bank activity regularly and you've noticed some odd, small transactions that you fail to identify, then your account could already be hacked. Sometimes hackers will take small amounts or purchase inexpensive items to check the validity of an account before emptying the vault as it were. Contact your bank immediately.

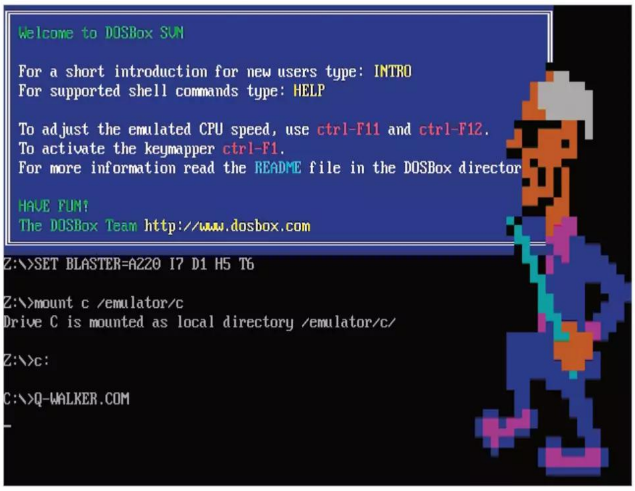


All Transactions

DATE ▲	DESCRIPTION	TYPE ?	IN (£)	OUT (£)	BALANCE (£)
View Pending Transactions					+
22 Feb 17	SAVE THE CHANGE	BP		0.30	125.00
21 Feb 17	OASIS DENTAL CARE	DEB		19.70	125.30
20 Feb 17	NEXT DIRECTORY CAT	FPO		40.00	145.00
20 Feb 17	J SLOCOMBE	TFR	40.00		185.00
20 Feb 17	D M CUMMINGS	FPO		55.00	145.00

SLOW PC

One of the many signs of your computer being infected by a virus is the sudden slowing down of the overall system. Most operating systems, Windows in particular, slow down over time but if you power up your computer one day and it's noticeably slower than usual we'd recommend you run a virus scan.



```
Welcome to DOSBox SVN

For a short introduction for new users type: INTRO
For supported shell commands type: HELP

To adjust the emulated CPU speed, use ctrl-F11 and ctrl-F12.
To activate the keymapper ctrl-F1.
For more information read the README file in the DOSBox director

HAVE FUN!
The DOSBox Team http://www.dosbox.com

Z:\>SET BLASTER=A220 I7 D1 H5 T6

Z:\>mount c /emulator/c
Drive C is mounted as local directory /emulator/c/

Z:\>c:

C:\>Q-WALKER.COM
_
```

SLOW BROWSER

In relation to the previous tip, a browser slow down can also indicate that something is potentially going on. Browser hijacking can adversely affect the speed at which pages load, as it's sending information to a remote source. Naturally it's not always a digital security issue but to make sure, check your system.

110101 NAME ADRES
LIN 101 Browser hijack
1101010 NAME ADRES

POP-UPS

Furthering the browser issue, if you suddenly notice a lot more advertising, pop-ups or similar, then it's usually a good sign that you're infected with some form of adware or Trojan tracker.

XEROX
WIN an $11,000
$999
INSWEB
Before you go, did you know....
You can add AOL for Broadband to any high-speed cable or DSL connection!
GET A FREE TRIAL!
TRY 2 RISK-FREE ISSUES!
What's New
15 FREE POWER GUIDES
Are You Paying Too
Rates are at Hist
TRAVELZOO

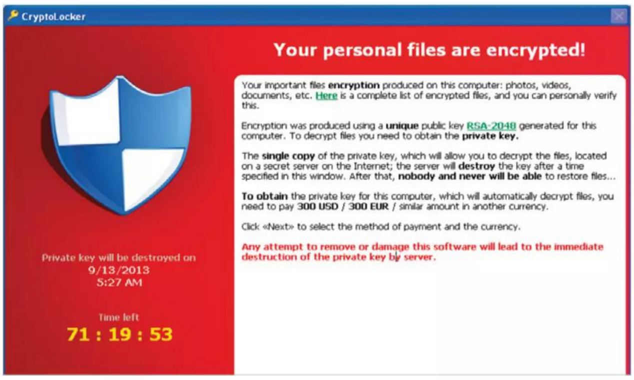
INFECTED CONTENT

Viruses want to be spread from one computer to another and they can infect your email or social media platforms. If you suddenly have your friends asking you why you're posting adverts for pharmaceutical enhancements, then there's a good chance you're infected with something.

Special Delivery

RANSOMWARE WARNING

In the case of a ransomware attack, you don't often get much warning that something is about to happen. Generally speaking, a sudden and inexorable slowing down of your computer will be a key element, as the ransomware is frantically encrypting your files in the background.


CryptoLocker

Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt files you need to obtain the **private key.**

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **300 USD / 300 EUR** / similar amount in another currency.

Click «Next» to select the method of payment and the currency.

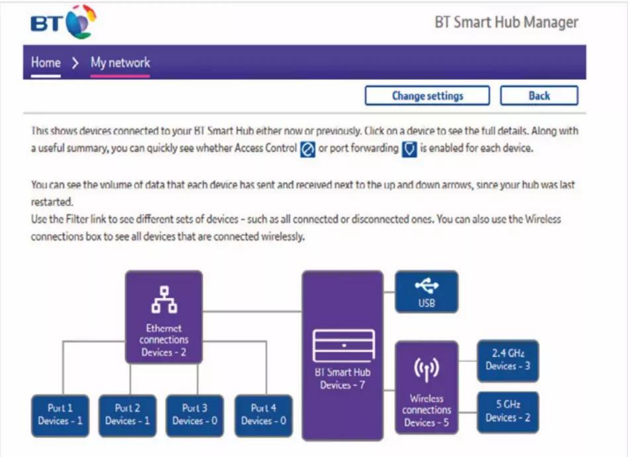
Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Private key will be destroyed on
9/13/2013
5:27 AM

Time left
71 : 19 : 53

ROUTER LOGS

It's always recommended to check your router's logs frequently. Although hackers are generally anonymous groups or individuals on the other side of the world, often a hacker could simply be a neighbour leeching your broadband connection. Check the logs for any unidentifiable computers attaching to the router.

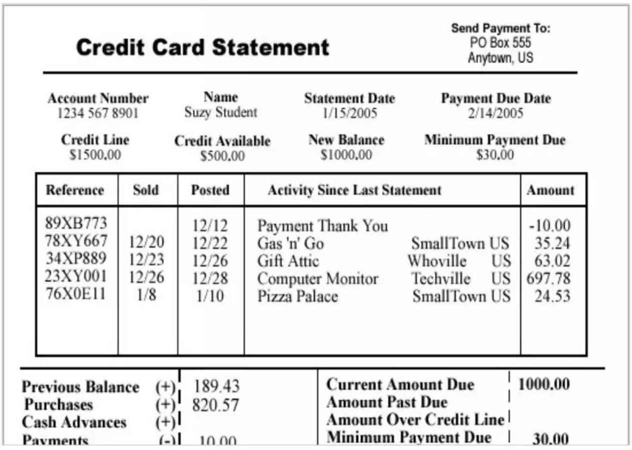

BT
BT Smart Hub Manager
Home
My network
Change settings
Back
Ethernet connections Devices - 2
BT Smart Hub Devices - 7
USB
Wireless connections Devices - 5
2.4 GHz Devices - 3
5 GHz Devices - 2
Port 1 Devices - 1
Port 2 Devices - 1
Port 3 Devices - 0
Port 4 Devices - 0

This shows devices connected to your BT Smart Hub either now or previously. Click on a device to see the full details. Along with a useful summary, you can quickly see whether Access Control or port forwarding is enabled for each device.

You can see the volume of data that each device has sent and received next to the up and down arrows, since your hub was last restarted.
Use the Filter link to see different sets of devices - such as all connected or disconnected ones. You can also use the Wireless connections box to see all devices that are connected wirelessly.

BANK STATEMENTS

Keeping an eye on your credit card statements will reveal any compromising security leaks. Just as with bank statements, small transactions are usually the first indicator, then once the hacker knows the card is valid they can then blitz it until you've run up a huge debt. Always check your statements and mark any suspicious transactions.



Credit Card Statement

Send Payment To:
PO Box 555
Anytown, US

Account Number	Name	Statement Date	Payment Due Date
1234 567 8901	Suzy Student	1/15/2005	2/14/2005
Credit Line	**Credit Available**	**New Balance**	**Minimum Payment Due**
$1500.00	$500.00	$1000.00	$30.00

Reference	Sold	Posted	Activity Since Last Statement		Amount
89XB773		12/12	Payment Thank You		-10.00
78XY667	12/20	12/22	Gas 'n' Go	SmallTown US	35.24
34XP889	12/23	12/26	Gift Attic	Whoville US	63.02
23XY001	12/26	12/28	Computer Monitor	Techville US	697.78
76X0E11	1/8	1/10	Pizza Palace	SmallTown US	24.53

Previous Balance	(+)	189.43	**Current Amount Due**	**1000.00**
Purchases	(+)	820.57	**Amount Past Due**	
Cash Advances	(+)		**Amount Over Credit Line**	
Payments	(-)	10.00	**Minimum Payment Due**	**30.00**

Top Ten Antivirus and Security Packages

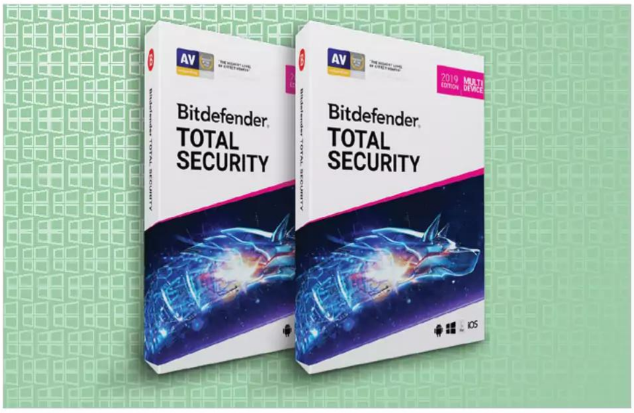
While the built-in Windows Defender is a great antivirus and security tool, it's nowhere near as capable as one of the many third-party security suites. The likes of Bitdefender, McAfee and Symantec have years of security specialism behind their products.

Better Protection

A third-party security suite offers much than virus scanning. With one of these, you're covered against most, if not all, digital threats. Here are ten security suites worth considering if you're serious about your digital protection.

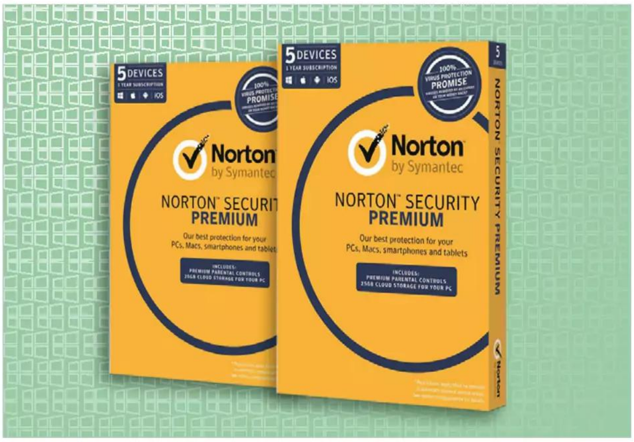
BITDEFENDER

Bitdefender Total Security 2019 is the latest security suite from one of the world's leading security specialists. This version offers unrivalled levels of protection and performance for Windows, macOS and Android platforms. There's even an advanced ransomware protection element to help protect your folders.


Bitdefender
TOTAL SECURITY
2019 EDITION
MULTI DEVICE

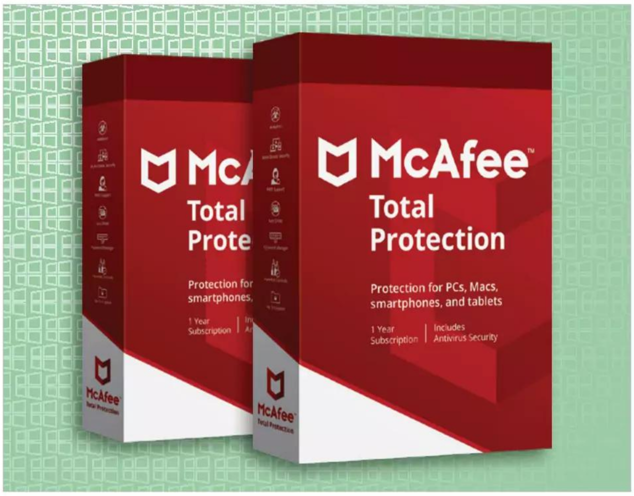
SYMANTEC

Norton Security Premium is Symantec's top choice for the home user. With it, you can protect up to ten PCs, Macs, smartphones, or tablets and it'll keep you safe when shopping online, general surfing, or when conducting transactions.


5 DEVICES
1 YEAR SUBSCRIPTION
100% VIRUS PROTECTION PROMISE
Norton by Symantec
NORTON SECURITY PREMIUM
Our best protection for your PCs, Macs, smartphones and tablets
INCLUDES: PREMIUM PARENTAL CONTROLS 25GB CLOUD STORAGE FOR YOUR PC

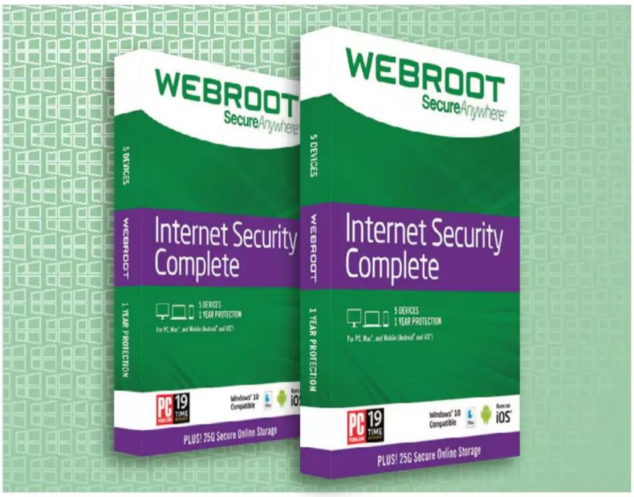
MCAFEE

McAfee Total Protection offers a 100% guarantee of virus removal, or you get your money back. There are three main versions available: Antivirus Plus, Total Protection and Livesafe, each has its own particular twist, but all offer excellent security features and benefits.


McAfee
Total Protection
Protection for PCs, Macs, smartphones, and tablets
1 Year Subscription
Includes Antivirus Security

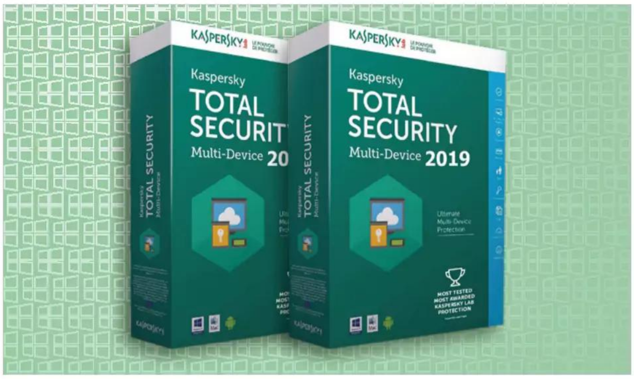
WEBROOT

Out of the three possible solutions available from Webroot, Webroot Internet Security Complete is the one to consider for home users. With it, you're protected from virtually any threat, as well as offering 25GB of secure online cloud storage.


WEBROOT SecureAnywhere
5 DEVICES
Internet Security Complete
1 YEAR PROTECTION
PLUS! 25G Secure Online Storage

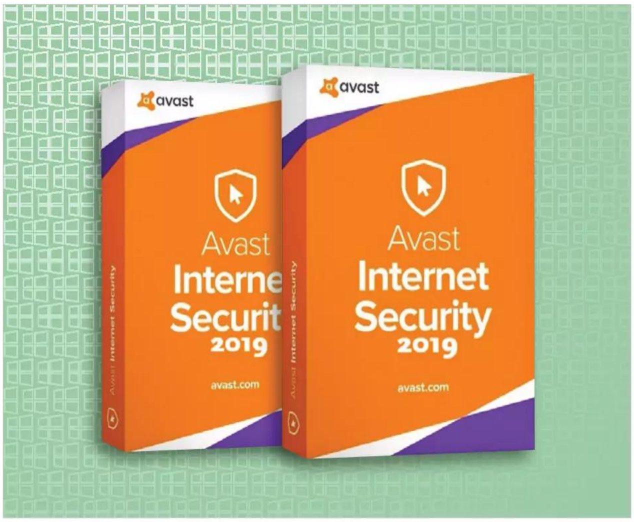
KASPERSKY

Kaspersky's Total Security 2019 is one of the best go-to products available on the market. It's great value for money and offers superb protection for your PC and other devices. You get parental controls, secure password storage, encryption and identity protection all under a single security suite.


KASPERSKY
Kaspersky
TOTAL SECURITY
Multi-Device 2019

AVAST

Avast has offered free antivirus software for many years, but its other products: Internet Security and Premier, are also well worth looking into. With both versions, you'll get online banking protection, identity protection and email protection, all for a reasonable cost too.


avast
Avast
Internet
Security
2019
avast.com

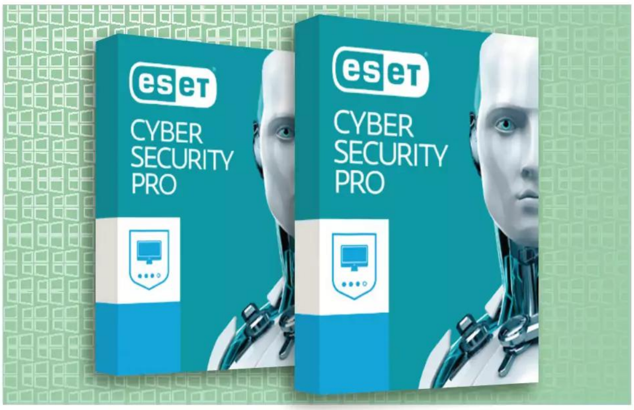
EMSISOFT

Emsisoft Internet Security is an award-winning security suite that offers plenty of great features and elements. It's quick, easy to use, cost effective and does an excellent job at protection you and your devices from modern security threats.

EMSISOFT
INTERNET SECURITY
FIREWALL

ESET

ESET Internet/Cyber Security is a comprehensive protection package for everyday users. It offers online banking protection, alerts for any malicious attempts to control your webcam and a fine-tuned balance between security and privacy.


eset
CYBER
SECURITY
PRO

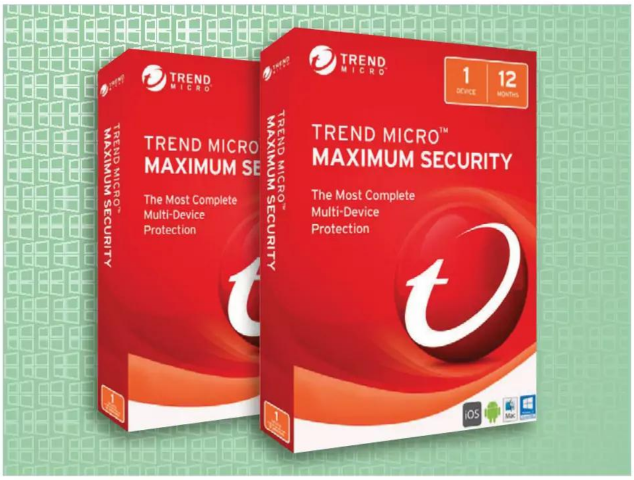
F-SECURE

F-Secure has been in the security and protection business for a lot of years and as such, its products are often considered one of the best available. F-Secure Total is the top choice for the home user, as not only does it provide superb antivirus protection, it also offers a Virtual Private Network (VPN) for added privacy when online.

F-Secure
TOTAL SECURITY AND PRIVACY
Internet security and VPN for all devices

TREND MICRO

Trend Micro Maximum Security offers superlative protection for up to five different devices along with extended protection for children, Internet passwords and privacy on social media sites. It's great value for money and performs excellently too.


TREND MICRO
TREND MICRO™
MAXIMUM SECURITY
The Most Complete Multi-Device Protection
1 DEVICE
12 MONTHS

Bitdefender Total Security 2019 Review

Bitdefender is regarded as one of the best antivirus and security companies in the world. Its products have won numerous awards and have been proved time and time again to be efficient and effective whilst offering cutting edge technology.

The Ultimate Protection

There's a lot to offer from Bitdefender's Total Security 2019. It's one of the leading security suites available and is cited as possibly the best total protection package in the world. Let's see what it has to offer.

Total Security 2019 is Bitdefender's flagship product and offers comprehensive security packages for Windows, macOS and Android users, all under a single web portal. Pricing does alter slightly, depending on what special deal may be available, but expect to pay somewhere in the region of £69.99 for a single year license for up to five devices.

What do you get for your money? Well, Bitdefender has upped the ante with regards to its protection suite, not an easy task for a company with a long history of already providing the leading security suite on the market. Total Security 2019 is quick, easy to install and understand, with the unboxing to installation and a complete system scan taking no more than half an hour.

Most of the problem with modern security suites is the heavy interface that comes with the package. A modern suite must include a wealth of elements to make it even slightly competitive in an already saturated and quite aggressive marketplace. This in turn creates an interface that's often too cluttered and a little overwhelming for the newcomer. Bitdefender though, has managed to package together a clean and sleek setup, with the most prominent features available, with just a click or a couple of clicks of the mouse.

Naturally you can dig much deeper into the settings, selecting pre-defined profiles and modes, or tweaking the core to either lighten the security, without compromising the overall defences, or tightening everything up to an almost NSA-level of security clearance.

It's packed full of interesting and useful features, some of which you never thought you'd appreciate until you actually had them to hand. For example, the vulnerability scanner will hunt down any missing Windows updates, issues with Wi-Fi security and even weak passwords. Integration with your browser is excellent, offering clearly defined green ticks next to search results that are classed as safe to visit, including integration with Facebook. You can also set up a secure vault for files that you want to mark as ultra-private and keep away from any prying eyes.

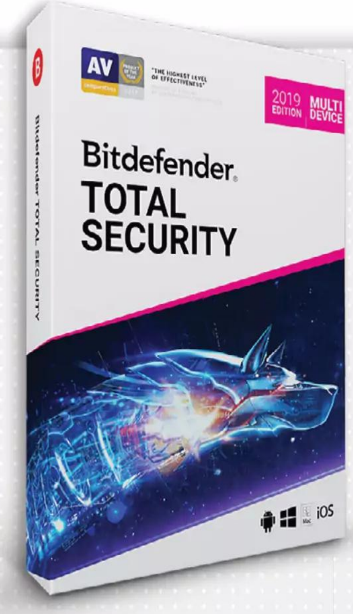
You'll command everything from the Bitdefender Central Activity Dashboard, which will display the current subscription, to the status of your Bitdefender installed devices, alerts, reports and so on. It's a simple interface that keeps the stuff you want to see prominent, while gently hiding the deeper information that only the more advanced user may be interested in viewing. Of course, should anything untoward happen to any of the Bitdefender installed devices, you'll receive the appropriate warning. Interestingly, should you activate the parental features on any of the devices, the dashboard will inform you of your child's online activity, visited sites and social media behaviour.

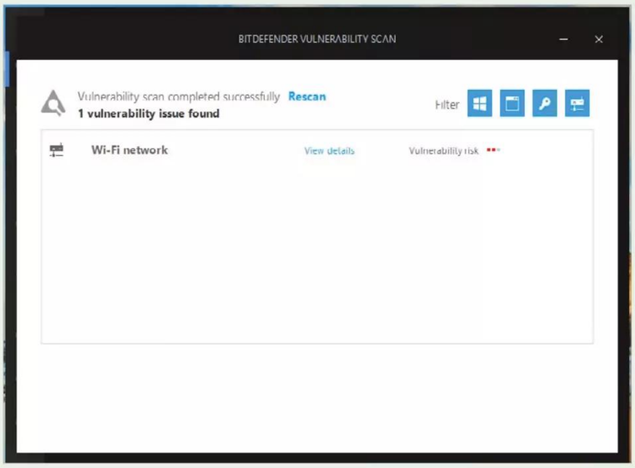
Ransomware is handled by an independent module that requires activation, once enabled it'll automatically protect files in your Documents folders, with the option to include other folders, too. Any attempt to edit one these protected files results in a message appearing, allowing you to confirm the action. This makes it increasingly difficult for ransomware to start encrypting and messing around with your valued data.

On top of all the superb features though, is the excellent scanning engine. The Bitdefender scan is quick and doesn't slow your computer down while being active in the background or while conducting a full system scan.

In short, if you're in the market for a complete and fully featured security suite, then Bitdefender Total Security 2019 is the one you should most definitely consider.

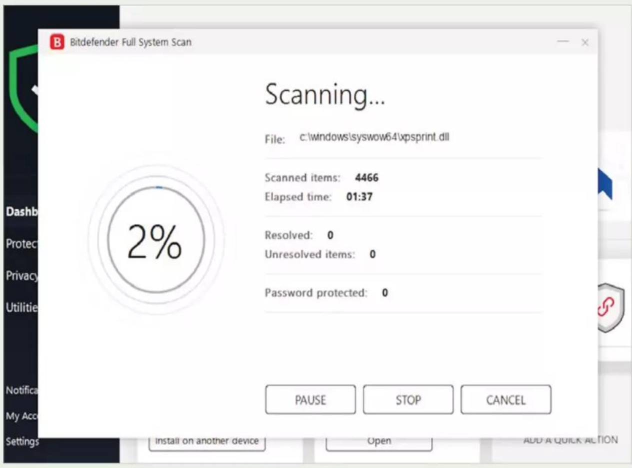
"Bitdefender Total Security 2019 is one of the best AV and protection products available today"


AV
"THE HIGHEST LEVEL OF EFFECTIVENESS"
2019 EDITION
MULTI DEVICE
Bitdefender
TOTAL SECURITY
Bitdefender TOTAL SECURITY
iOS


BITDEFENDER VULNERABILITY SCAN
Filter
Wi-Fi network
View details
Vulnerability risk

Vulnerability scan completed successfully Rescan
1 vulnerability issue found

"One of its many splendid features is a vulnerability scanner that informs you of any weaknesses in your system."


Bitdefender Full System Scan
2%
PAUSE
STOP
CANCEL

Scanning...

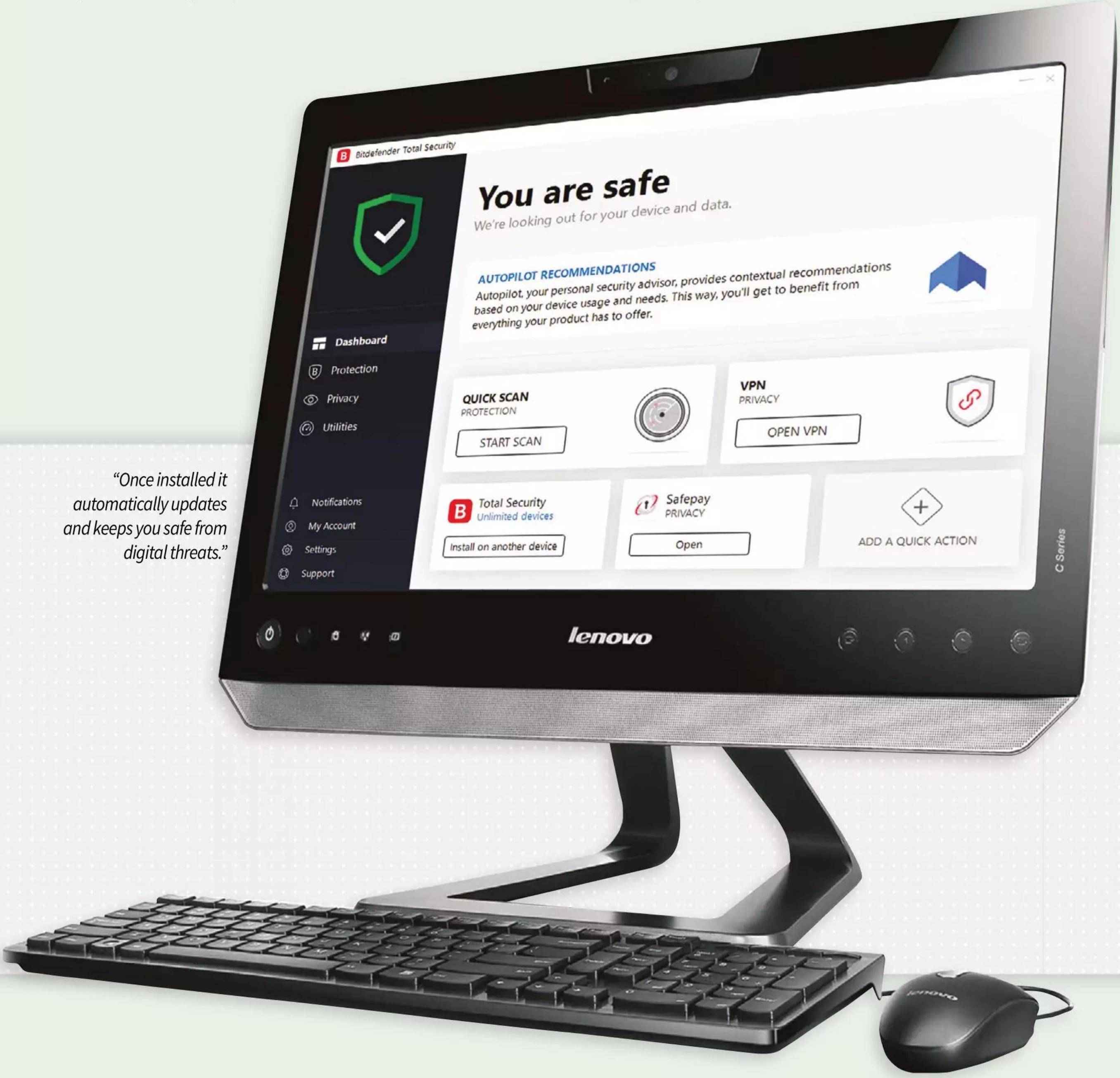
File: c:\windows\syswow64\xpsprint.dll

Scanned items: 4466
Elapsed time: 01:37

Resolved: 0
Unresolved items: 0

Password protected: 0

"The scanning engine is quick and efficient and doesn't unnecessarily slow your computer down."


Bitdefender Total Security
Dashboard
Protection
Privacy
Utilities
Notifications
My Account
Settings
Support
QUICK SCAN
PROTECTION
START SCAN
VPN
PRIVACY
OPEN VPN
Total Security
Unlimited devices
Install on another device
Safepay
PRIVACY
Open
ADD A QUICK ACTION
lenovo
C Series

You are safe
We're looking out for your device and data.

AUTOPILOT RECOMMENDATIONS
Autopilot, your personal security advisor, provides contextual recommendations based on your device usage and needs. This way, you'll get to benefit from everything your product has to offer.

"Once installed it automatically updates and keeps you safe from digital threats."

Kaspersky Total Security 2019 Review

Kaspersky was one of the first security companies to offer the end-user a cross platform AV protection suite, some years ago now. Since then, the company has improved its products staggeringly and as such is now one of the leading security suites available.

Next Generation Protection

There are a lot of features to like about Kaspersky Total Security 2019, all of which help you not only be protected from whatever's out there, but also better manage your system.

Kaspersky's Total Security 2019 is the mega-product of the company's AV and protection utilities for home users. It's reasonably priced at around £39.99 for one device plus a year's subscription, rising to a maximum of £109 for five devices and a two-year subscription. Obviously prices can change, depending on what deals are currently available, so check the Kaspersky website for the latest guide.

Much like the Bitdefender entry, Kaspersky has gone to great lengths to provide an easy to use and simple to understand interface. While, again like Bitdefender, you're able to delve deeper into the inner workings, the average user isn't instantly bewildered by pages upon pages of technical jargon, icons and sub-menus. It's handy too that everything starts from the Kaspersky online portal, where you'll download your purchased software, alongside installers for other modules that eventually all fall under the same umbrella control centre.

The front-end categories that are available via the control centre are: Scan, Database Update, Safe Money, Password Manager, Privacy Protection, Backup and Restore, Protection for all devices and Parental Control. Most are fairly self-explanatory, however, components such as Safe Money and Privacy Protection deserve a little more detail.

Safe Money utilises Kaspersky's unique protection engine, whereby your online transactions are safely behind the product's security web. This feature takes care of protecting your shopping, as well as online banking, so it's an impressive weapon in the already ample Kaspersky arsenal.

Privacy covers a range of different features. The core component protects you while surfing, guarding your online identity and information, while also actively blocking malicious websites and preventing any form of tracking or monitoring. It also includes an element that blocks any attempts to access your computer's webcam, which is certainly a handy feature and it'll block any attempts to access your stored data while you browse the Internet.

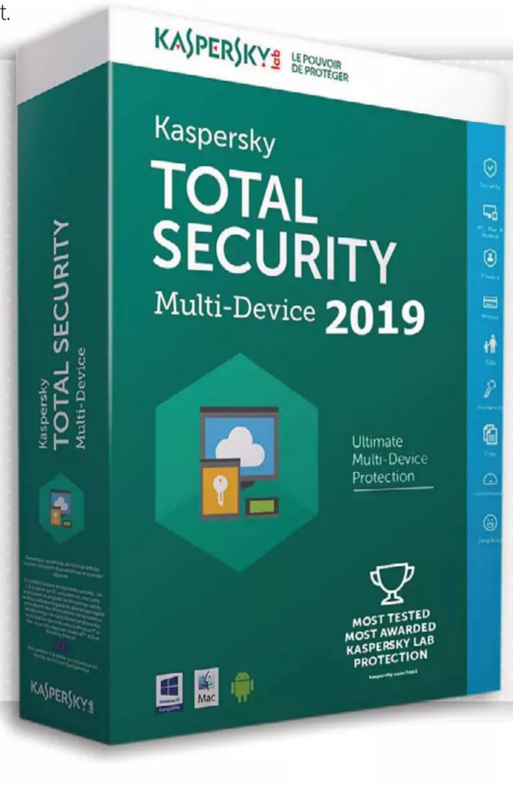
> *"Kaspersky Total Security 2019 is one of the leading AV and security products for the home user"*

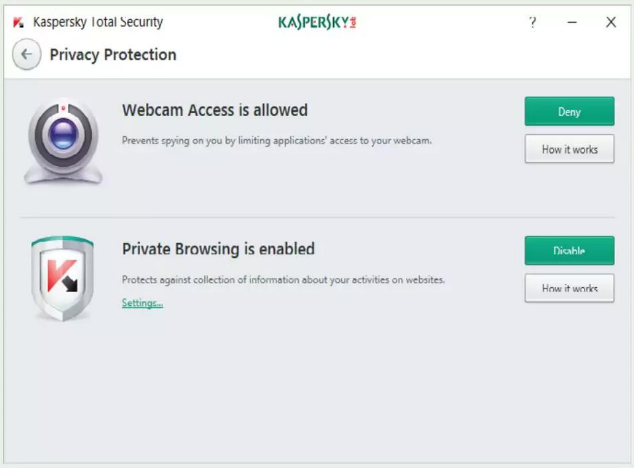
Needless to say, the features available are certainly impressive. Beyond the few we've mentioned above, there's also controls to improve browser security, protection for any cloud access, a vulnerability scanner and a trusted application mode that will only allow white-listed programs to be executed. You can create a Kaspersky Rescue Disk, which you're able to boot from should something ever go wrong, allowing you to scan and clean your computer without it needing to access Windows. The list goes on and covers pretty much everything you would want from an all-encompassing security suite.

In terms of speed of operation and the performance hit on the system, Kaspersky Total Security 2019 is about on par with that of Bitdefender. Admittedly, It's not as fast at completing a full system scan, but it's only a minute or so out. The performance hit on the system is negligible; in fact, you'll be hard-pressed to notice any negative impact once the software is installed and continually scanning.

One last component worth mentioning is the Parental Control feature. With this, Kaspersky offers a method of keeping children safe while they use their devices. You can create usage scheduling, GPS safe zones and receive notifications should anything suspicious attempt to access your child's device when they're using it. Beyond that, there are also filters to stop children accessing adult sites, or sites that can feature disturbing content.

Kaspersky Total Security 2019 is an impressive product and one that the home user can certainly feel confident about. It's quick, easy to use, regularly updated and ticks all the right boxes from the point of view of a user, parent and someone who wants to make sure they're as secure as possible on the modern Internet.


KASPERSKY lab
LE POUVOIR DE PROTÉGER
Kaspersky
TOTAL SECURITY
Multi-Device 2019
Ultimate Multi-Device Protection
MOST TESTED MOST AWARDED KASPERSKY LAB PROTECTION


Kaspersky Total Security
KASPERSKY
?
–
X
Privacy Protection
Deny
How it works
Disable
How it works
Settings...

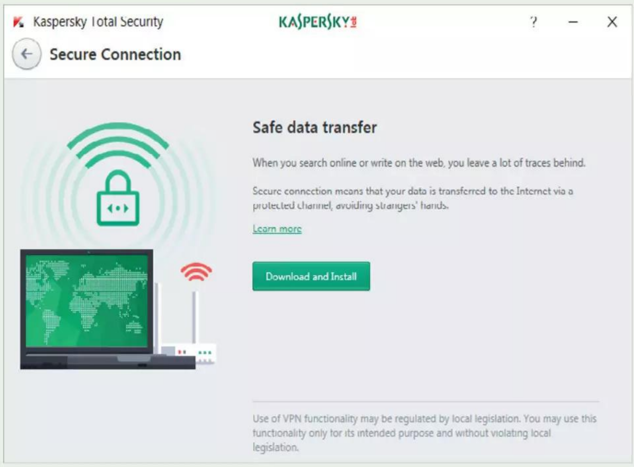
Webcam Access is allowed

Prevents spying on you by limiting applications' access to your webcam.

Private Browsing is enabled

Protects against collection of information about your activities on websites.

"Components such as Privacy Protection are welcomed and remarkably useful to the end user."


Kaspersky Total Security
KASPERSKY
?
–
X
Secure Connection
Learn more
Download and Install

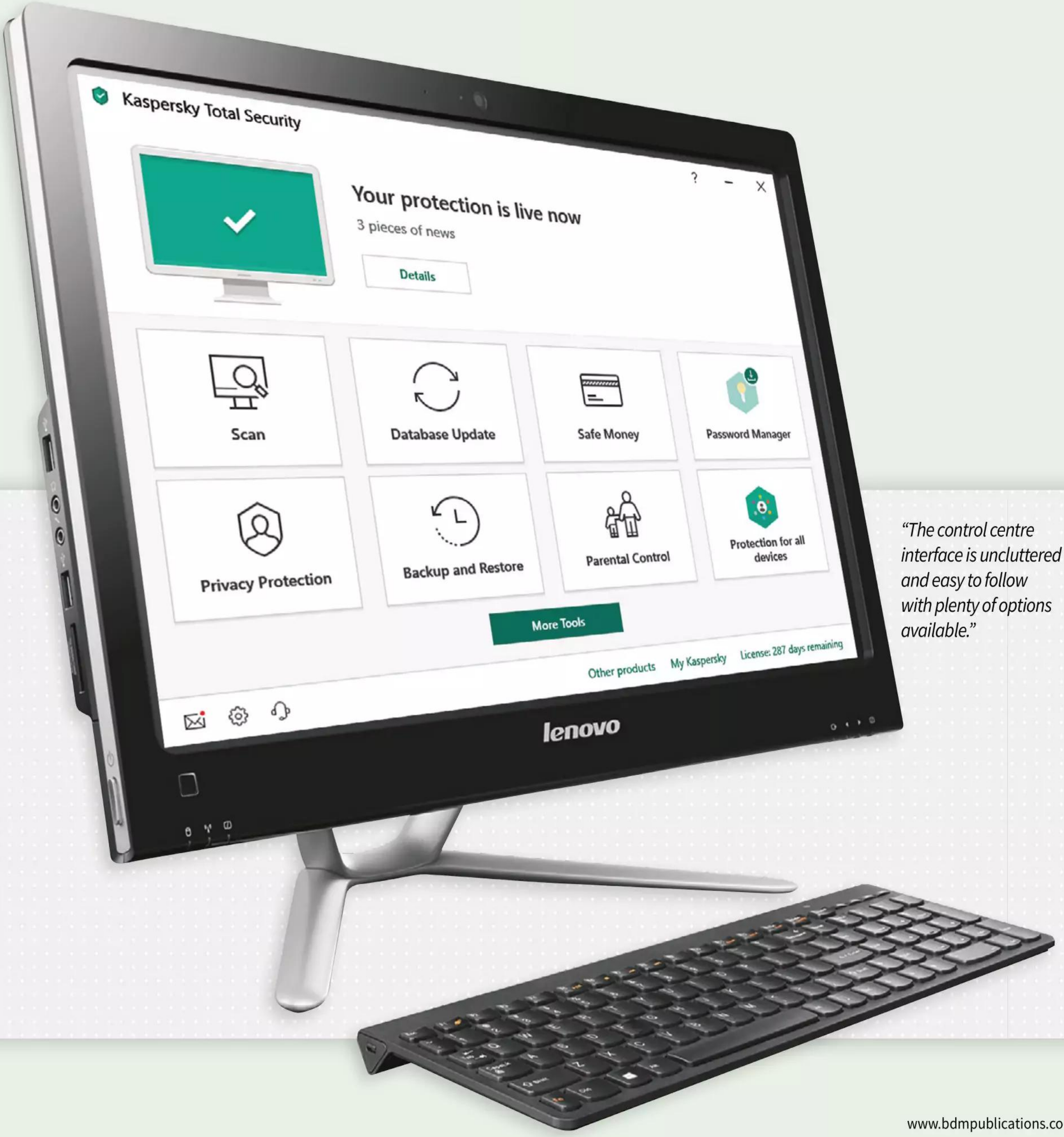
Safe data transfer

When you search online or write on the web, you leave a lot of traces behind.

Secure connection means that your data is transferred to the Internet via a protected channel, avoiding strangers' hands.

Use of VPN functionality may be regulated by local legislation. You may use this functionality only for its intended purpose and without violating local legislation.

"There's a lot to like about Kaspersky's flagship product. It's quick, easy to use and ticks all the right boxes."


Kaspersky Total Security
?
–
X
Details
Scan
Database Update
Safe Money
Password Manager
Privacy Protection
Backup and Restore
Parental Control
Protection for all devices
More Tools
Other products
My Kaspersky
lenovo

Your protection is live now

3 pieces of news

License: 287 days remaining

"The control centre interface is uncluttered and easy to follow with plenty of options available."

McAfee Total Protection Review

The name McAfee has been synonymous with antivirus and security since the late '80s and is considered as the granddaddy of the computer security world. Its latest complete protection package, Total Protection, has a lot to offer the end user, as you'll soon see.

McAfee For Consumers

McAfee is now a part of Intel Security and as such it's backed by the latest generation of hardware level security as well as it's award winning software scanning engine.

The name McAfee has seen some interesting press over the last decade, not just from the security software itself, but also with regards to the company founder, John McAfee. The founder's colourful lifestyle aside, McAfee Total Protection is a singularly impressive suite of tools. The cost is a little higher than the previous entries, priced at £89.99 for a year's subscription (though, regional and special offers will reduce that amount considerably). However, one highlighted feature is the Virus Protection Pledge, whereby your money is refunded should McAfee not be able to remove a virus that's already on your computer.

It's worth mentioning that the annual subscription includes installation on an unlimited number of devices; which is certainly worth considering if you're one of the many modern households that owns countless Internet-connected devices, computers and everything in-between. It's without doubt, an excellent choice for the home user.

Both installation and the initial full system scan were slower than that of Bitdefender and Kaspersky, but only by about five minutes. If you're constantly in a rush you may want to consider the other suites, however, most users will be satisfied with the result from McAfee – at any rate, it gives you time to make a cup of tea while you're waiting for the scan to finish.

As with the other products we've looked at, the interface is simple to understand and navigate, with the core and most used functions within easy reach of the mouse pointer, while the more advanced options are neatly tucked away for those who are a little more knowledgeable about such things. In short, it works well and keeps the wealth of available options at bay until the user requests them. Needless to say, the settings are extensive, allowing the advanced user a higher degree of control over the way the suite of tools works within the system on which it's installed.

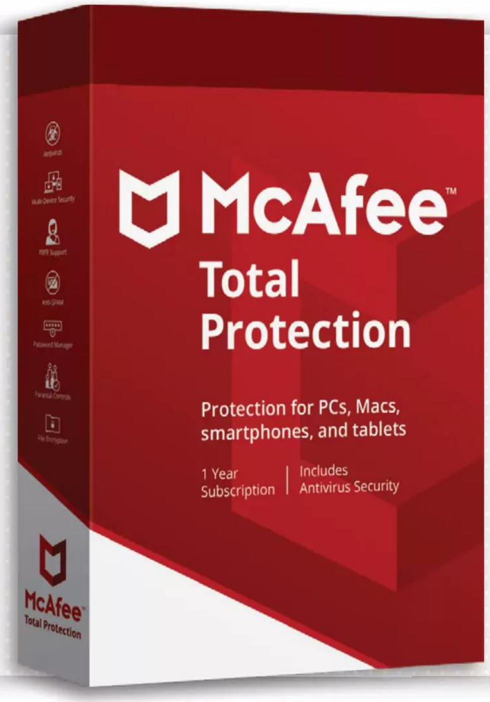
McAfee's three-tiered approach to system protection is worthy of mentioning. First, the scanning technology does a thorough, fine-toothed comb inspection of the files on the system. Heuristic analysis then takes over, monitoring: behaviour of files, functions and even code inspection, to check for possible unknown viruses based on the way they work. Lastly, anything that's even remotely suspicious is automatically uploaded to the McAfee Global Threat Intelligence Lab for analysis. Should the code prove to be a new form of virus, the team behind the impressive sounding lab will create a fix and push it out to the other two hundred million plus McAfee users. It's not nice getting a computer virus, but at least with McAfee you can be assured that your misfortune is helping others.

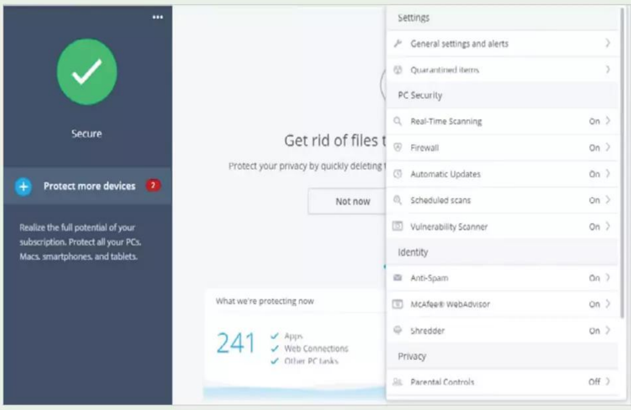
The Password Management feature is an interesting addition to the McAfee suite of tools. In reality, it's Intel's True Key Security component that, although not the top of the league password management program, does boast a multi-factor authentication process. In addition, you can set individual True Key passwords for all members of family - up to five users.

Among the multitude of features, you'll find File Lock an interesting addition. This is an impressive encryption mechanism that'll lock your files behind an impenetrable, military grade encryption wall. It's not activated by default, which is understandable as encryption does still carry with it a higher level of user knowledge and it's not something the average user will immediately consider adopting when setting up their computer security.

As for performance, we've already mentioned that McAfee is somewhat slower than that of Bitdefender or Kaspersky, but as with the other entries, you won't notice any perceivable slowdown in the computer's operation with it installed. McAfee Total Protection does an excellent job of keeping your files and personal information safe when online and with its added features it's certainly worth looking into at greater depth.

"McAfee Total Protection, now a part of Intel Security, is certainly worth considering for the home user."


McAfee
Total Protection
Protection for PCs, Macs, smartphones, and tablets
1 Year Subscription
Includes Antivirus Security

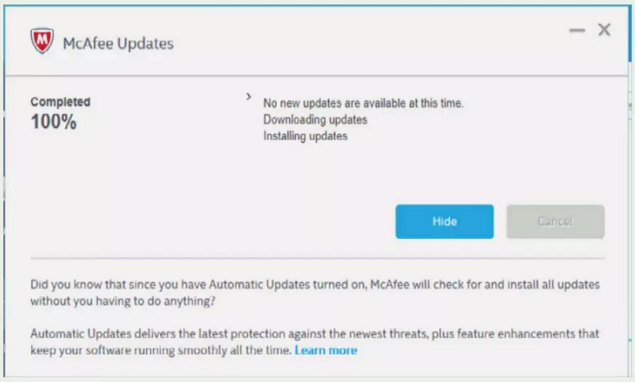

Secure
Protect more devices
2
Get rid of files t
Not now
What we're protecting now
241
Apps
Web Connections
Other PC tasks
Settings
General settings and alerts
Quarantined items
PC Security
Identity
Privacy

Realize the full potential of your subscription. Protect all your PCs, Macs, smartphones, and tablets.

Protect your privacy by quickly deleting t

Real-Time Scanning On
Firewall On
Automatic Updates On
Scheduled scans On
Vulnerability Scanner On
Anti-Spam On
McAfee® WebAdvisor On
Shredder On
Parental Controls Off

"McAfee is simple to use, update and monitor. Plus the added bonus of unlimited device installation is an alluring factor."


McAfee Updates
Hide
Cancel
Learn more

Completed
100%

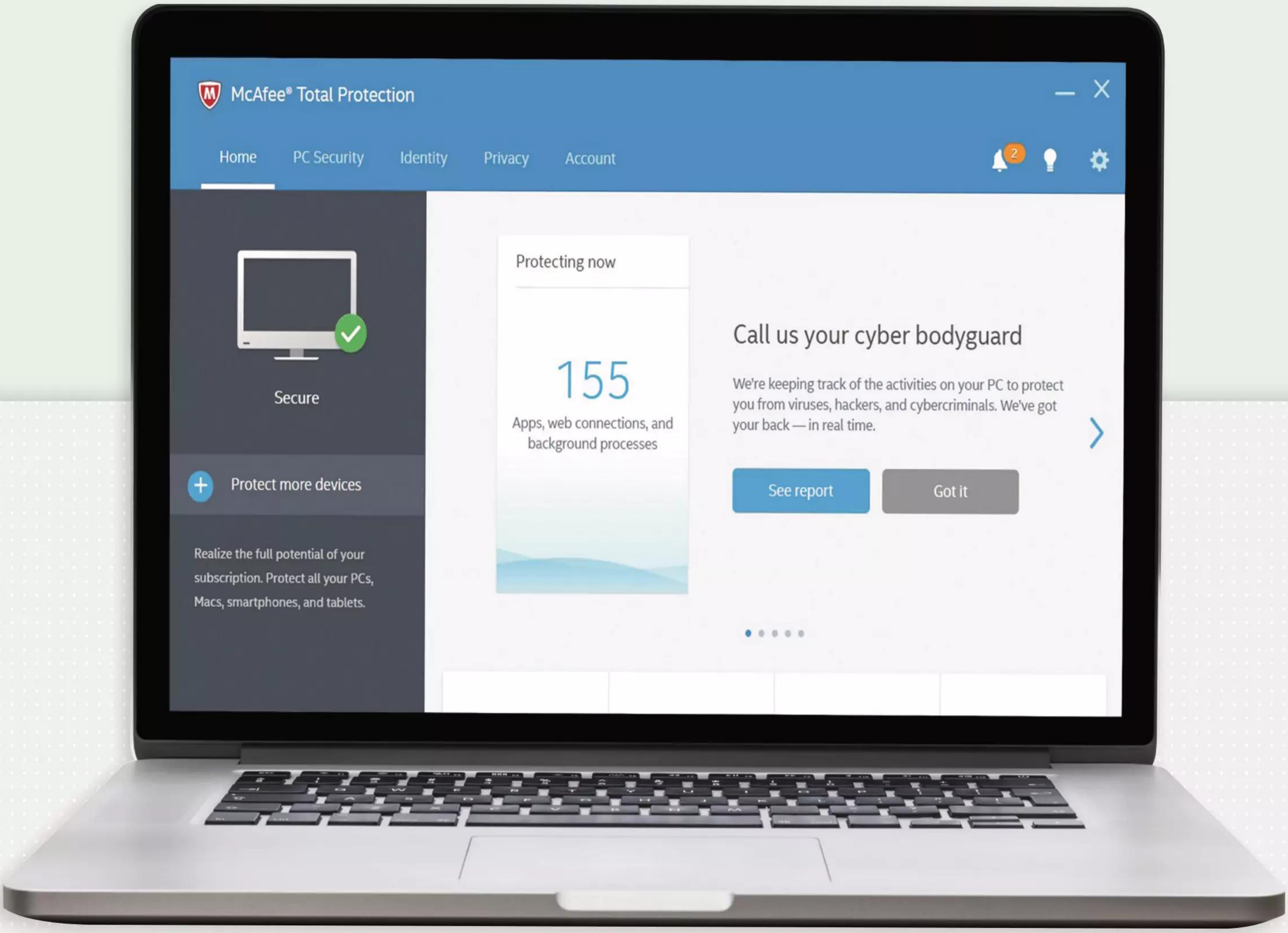
No new updates are available at this time.
Downloading updates
Installing updates

Did you know that since you have Automatic Updates turned on, McAfee will check for and install all updates without you having to do anything?

Automatic Updates delivers the latest protection against the newest threats, plus feature enhancements that keep your software running smoothly all the time. Learn more

"There are ample features to explore and utilise to improve your security when online."

"The scanning isn't as quick as the other products we've looked at but it's certainly as effective."


McAfee® Total Protection
Home
PC Security
Identity
Privacy
Account
2
Secure
Protect more devices
Protecting now
155
See report
Got it

Realize the full potential of your subscription. Protect all your PCs, Macs, smartphones, and tablets.

Apps, web connections, and background processes

Call us your cyber bodyguard

We're keeping track of the activities on your PC to protect you from viruses, hackers, and cybercriminals. We've got your back — in real time.

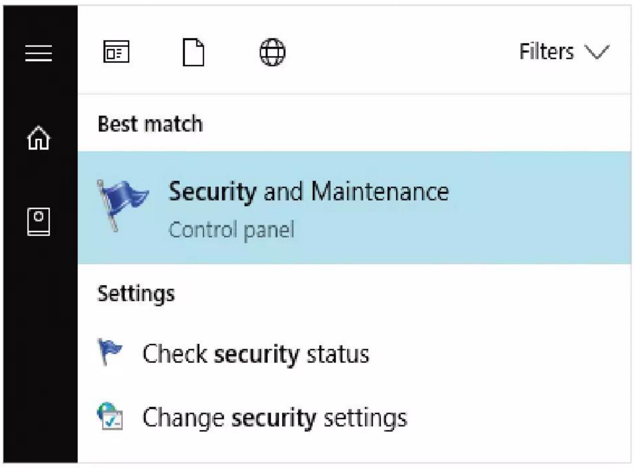
Setting Up Windows 10 Security

Before we dig deeper into the many levels of Windows 10 security features, it's worth taking a moment to check that the initial security features are in indeed up and running, and doing what they're supposed to.

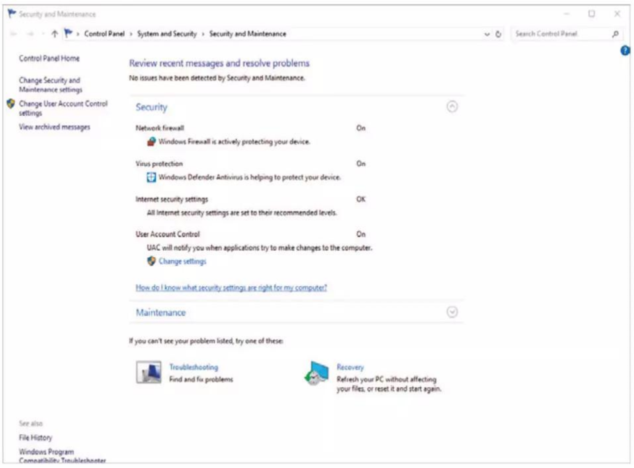
Are You Secure?

Remarkably, despite having an antivirus client installed, some users aren't even aware of the default Windows 10 security features. Here's a quick ten step process to check everything is working as it should.

STEP 1 Start by clicking on the Windows Start Button or pressing the Windows key on your keyboard. Enter security into the search bar and click the first option that appears in the results, Security and Maintenance.


Filters
Best match
Security and Maintenance
Control panel
Settings
Check security status
Change security settings

STEP 2 This will open the Security and Maintenance section of the Control Panel. There are two main sections within this page, click on the Security section to expand it. Ideally all the options within the Security section should be displaying On, with the exception of Internet Security Settings which will display OK.


Security and Maintenance
Control Panel › System and Security › Security and Maintenance
Search Control Panel
Control Panel Home
Change Security and Maintenance settings
Change User Account Control settings
View archived messages
See also
File History
Windows Program Compatibility Troubleshooter

Review recent messages and resolve problems

No issues have been detected by Security and Maintenance.

Security

Network firewall On
Windows Firewall is actively protecting your device.

Virus protection On
Windows Defender Antivirus is helping to protect your device.

Internet security settings OK
All Internet security settings are set to their recommended levels.

User Account Control On
UAC will notify you when applications try to make changes to the computer.
Change settings

How do I know what security settings are right for my computer?

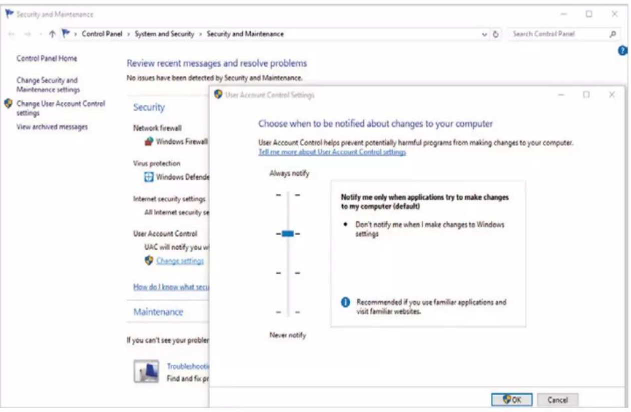
Maintenance

If you can't see your problem listed, try one of these:

Troubleshooting
Find and fix problems

Recovery
Refresh your PC without affecting your files, or reset it and start again.

STEP 3 Should any of the options display No, then you'll need to check the setting relating to that particular feature. For example, if your User Account Control (UAC) is set to Off, click the Change Settings link under the UAC option. The other features can be found via a search from the Windows Start Button.


Security and Maintenance
Control Panel › System and Security › Security and Maintenance
Search Control Panel
Control Panel Home
Change Security and Maintenance settings
Change User Account Control settings
View archived messages
Review recent messages and resolve problems
No issues have been detected by Security and Maintenance.
Security
Network firewall
Windows Firewall
Virus protection
Windows Defende
Internet security settings
All Internet security se
User Account Control
UAC will notify you w
Change settings
How do I know what secu
Maintenance
If you can't see your probler
Troubleshooti
Find and fix pr
User Account Control Settings
Always notify
Never notify
OK
Cancel

Choose when to be notified about changes to your computer

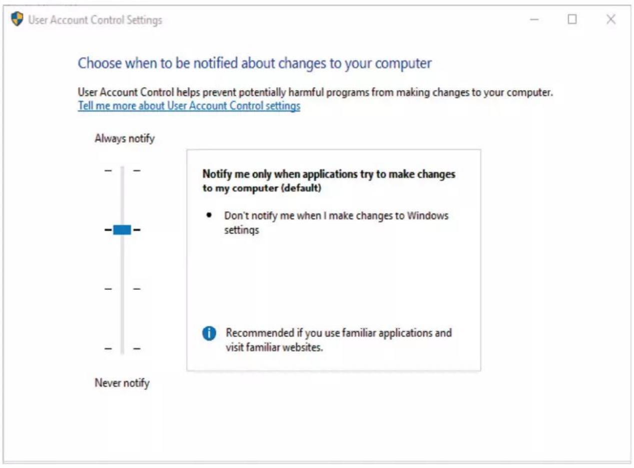
User Account Control helps prevent potentially harmful programs from making changes to your computer.
Tell me more about User Account Control settings

Notify me only when applications try to make changes to my computer (default)

- Don't notify me when I make changes to Windows settings

Recommended if you use familiar applications and visit familiar websites.

STEP 4 UAC will warn you of any attempt to access a system critical file. If any malware wants to alter a file, then you're asked if you want to proceed; obviously you don't, so you can say no and investigate the issue. There are various settings to choose from but the second step down from the top is the recommended.


User Account Control Settings
Always notify
Never notify

Choose when to be notified about changes to your computer

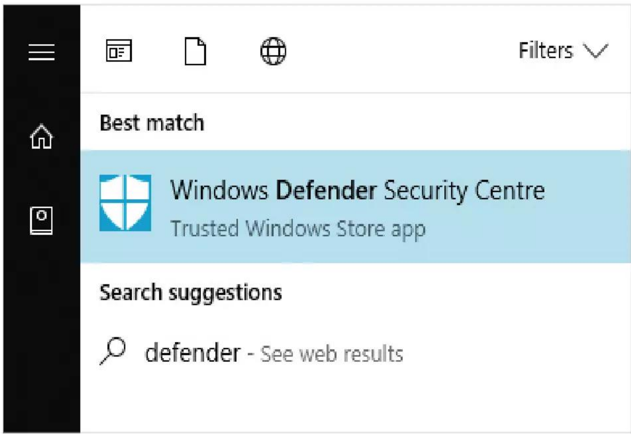
User Account Control helps prevent potentially harmful programs from making changes to your computer.
Tell me more about User Account Control settings

Notify me only when applications try to make changes to my computer (default)

- Don't notify me when I make changes to Windows settings

Recommended if you use familiar applications and visit familiar websites.

STEP 5 Close down the Security and Maintenance window, then click the Windows Start Button and search for Defender. Click the resulting Windows Defender Security Centre option.

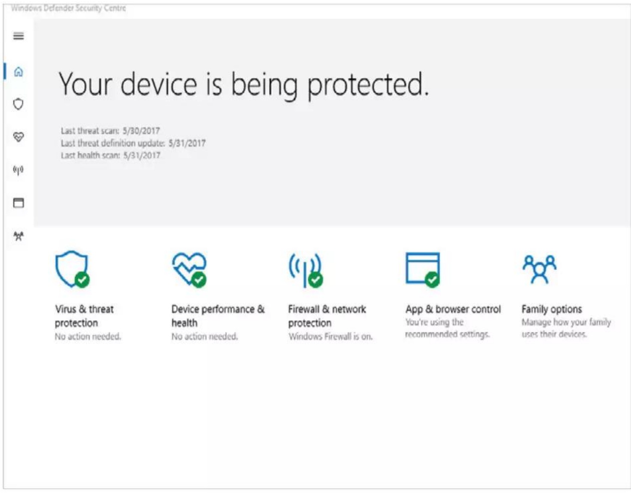

Filters
Best match

Windows Defender Security Centre
Trusted Windows Store app

Search suggestions

defender - See web results

STEP 6 If you're not using a third-party security and AV suite, then you need to make sure that Windows Defender is activated and working. There are numerous options available in the new-look Creators Edition Windows update of Defender. Each can be selected with a mouse click and viewed separately.


Windows Defender Security Centre

Your device is being protected.

Last threat scan: 5/30/2017
Last threat definition update: 5/31/2017
Last health scan: 5/31/2017

Virus & threat protection
No action needed.

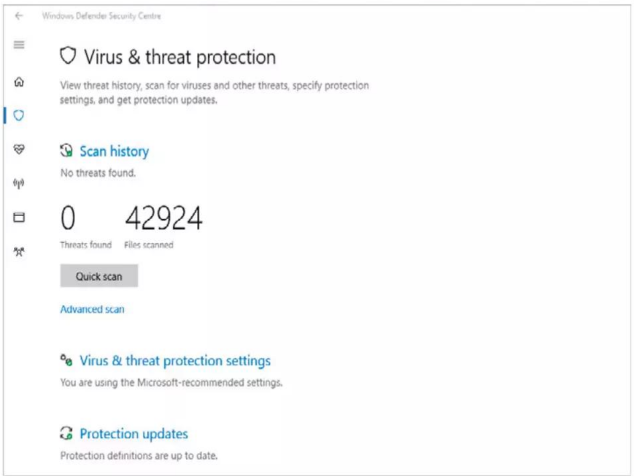
Device performance & health
No action needed.

Firewall & network protection
Windows Firewall is on.

App & browser control
You're using the recommended settings.

Family options
Manage how your family uses their devices.

STEP 7 Click the Virus & Threat Protection option. This will open a new window allowing you to perform a Quick or Full Scan of the system that details the number of threats found and the number of files scanned.


Windows Defender Security Centre

Virus & threat protection

View threat history, scan for viruses and other threats, specify protection settings, and get protection updates.

Scan history
No threats found.

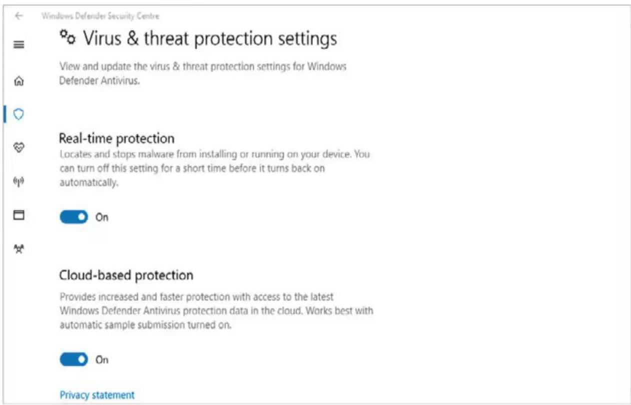
0 Threats found
42924 Files scanned

Quick scan
Advanced scan

Virus & threat protection settings
You are using the Microsoft-recommended settings.

Protection updates
Protection definitions are up to date.

STEP 8 If you click the Virus & Threat Protection Settings option, you can further opt to improve the system protection. Make sure that all the sub-options are set to On and scroll down to define the program's default Notifications.


Windows Defender Security Centre

Virus & threat protection settings

View and update the virus & threat protection settings for Windows Defender Antivirus.

Real-time protection
Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.

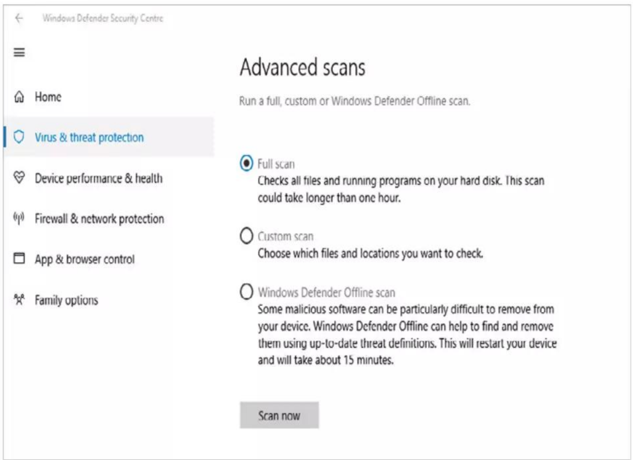
On

Cloud-based protection
Provides increased and faster protection with access to the latest Windows Defender Antivirus protection data in the cloud. Works best with automatic sample submission turned on.

On

Privacy statement

STEP 9 Returning to the main Virus & Threat Protection page, you can click the shield icon from the strip to the left of the screen; then click on the Advanced Scan link, located under the Quick Scan button. Within are options to run a Full System scan, a Custom scan (of a network location, for example) or an Offline scan.


Windows Defender Security Centre
Home
Virus & threat protection
Device performance & health
Firewall & network protection
App & browser control
Family options

Advanced scans

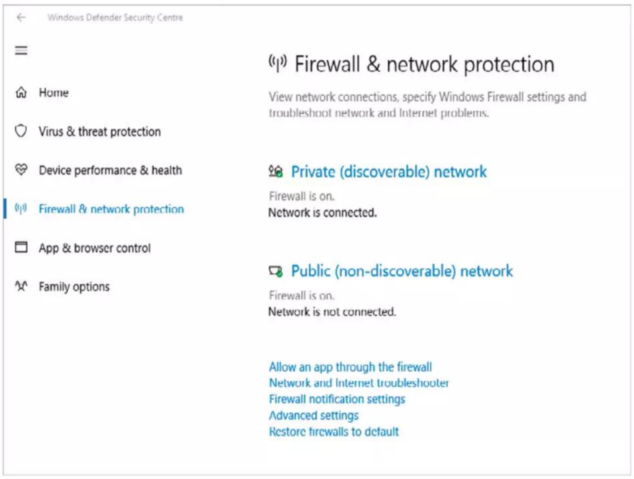
Run a full, custom or Windows Defender Offline scan.

● Full scan
Checks all files and running programs on your hard disk. This scan could take longer than one hour.

○ Custom scan
Choose which files and locations you want to check.

○ Windows Defender Offline scan
Some malicious software can be particularly difficult to remove from your device. Windows Defender Offline can help to find and remove them using up-to-date threat definitions. This will restart your device and will take about 15 minutes.

STEP 10 Lastly, click on the Firewall & Network Protection from the icon strip to the left. Again, if you're not using a dedicated, third-party security suite, make sure that the Private and Public Firewalls are set to on, thus protecting your system from unwanted intrusion.


Windows Defender Security Centre
Home
Virus & threat protection
Device performance & health
Firewall & network protection
App & browser control
Family options

Firewall & network protection

View network connections, specify Windows Firewall settings and troubleshoot network and Internet problems.

Private (discoverable) network
Firewall is on.
Network is connected.

Public (non-discoverable) network
Firewall is on.
Network is not connected.

Allow an app through the firewall
Network and Internet troubleshooter
Firewall notification settings
Advanced settings
Restore firewalls to default

Why Updating is Important

Continual updates, rebooting after an update has been installed, then the inevitable second reboot straight after the first to apply the update: it's little wonder people stray from the regular update checks. Whilst it can be a pain though, keeping things up to date is a top priority.

Update, reboot, update, reboot

Updates may well be the bane of the modern computer user but they are there for a reason. It's not the 8-bit era anymore, we need those updates to help protect our security. Here are 10 reasons why they're important.

PATCH VULNERABILITIES

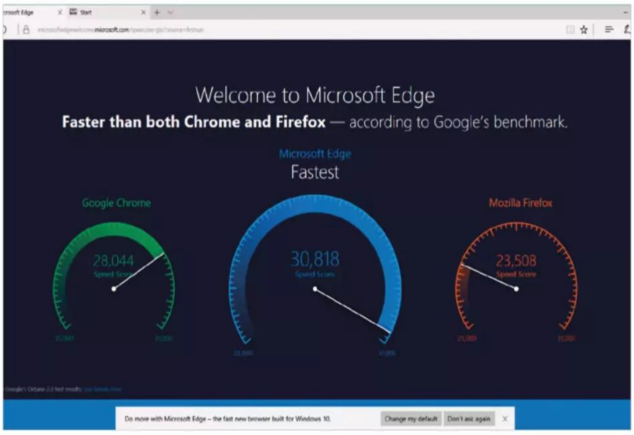
Windows updates patch recognised security holes in the core system. Many of the viruses around today exploit a vulnerability in the Windows code that hasn't been fixed yet. So when an update comes along, that potential flaw will be ironed out.

EXTRA SECURITY

In addition to potential security glitches in the code, often an update can contain an extra level of security that's been programmed in by the developers. For example, the code that handles remote desktop requests has had a security patch but another code that handles the authentication is hardened as a result.

BROWSER UPDATES

Windows 10 comes with many different programs to make it a more appealing environment. They include Internet Explorer and Edge browsers. As a part of Microsoft, these will need to be in tip-top working order to help prevent any modern Internet-borne viruses from entering the system. Daily update checks will keep things in shape.



Welcome to Microsoft Edge

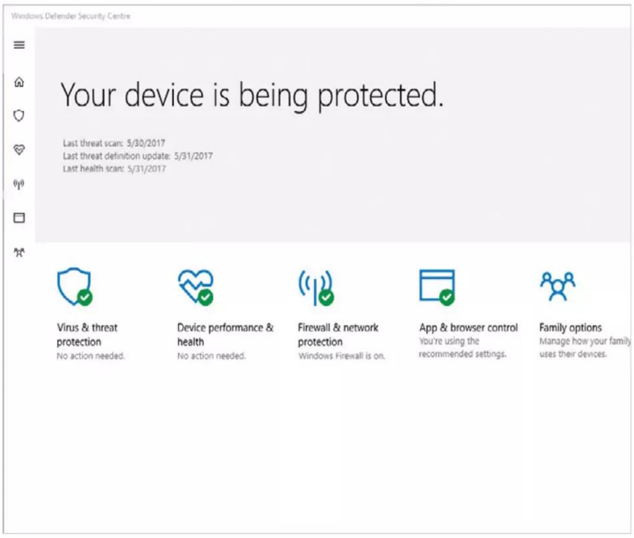
Faster than both Chrome and Firefox — according to Google's benchmark.

Do more with Microsoft Edge – the fast new browser built for Windows 10.

Start
Microsoft Edge
Fastest
Google Chrome
28,044
Speed Score
30,818
Speed Score
Mozilla Firefox
23,508
Speed Score
Change my default
Don't ask again

DEFENDER UPDATES

Windows Defender and its other security elements will require at least one update a day to keep up with the latest virus definitions. This is a much needed aspect of updating, as even if you only go online once every so often, being protected from locally spread malware (USB drives etc.) is equally important.



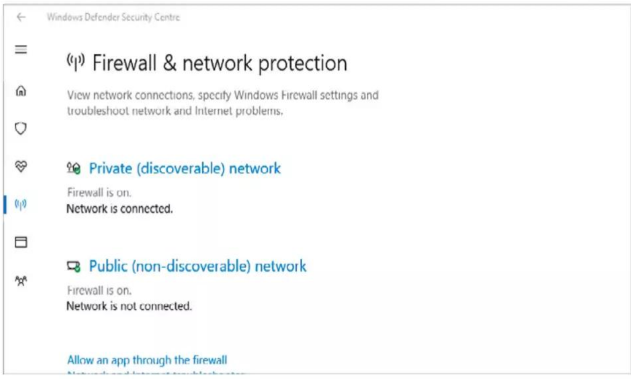
Your device is being protected.

Last threat scan: 5/30/2017
Last threat definition update: 5/31/2017
Last health scan: 5/31/2017

Windows Defender Security Centre
Virus & threat protection
No action needed.
Device performance & health
No action needed.
Firewall & network protection
Windows Firewall is on.
App & browser control
You're using the recommended settings.
Family options
Manage how your family uses their devices.

FIREWALL UPDATES

To expand the last reason, the Windows Firewall is one of the first layers of security on your system. With it, access to your computer from another source is monitored and even blocked, stopping potential threats before they even hit the virus defence layer. Updates make sure that the Firewall is up to scratch for the job.


Windows Defender Security Centre

Firewall & network protection

View network connections, specify Windows Firewall settings and troubleshoot network and Internet problems.

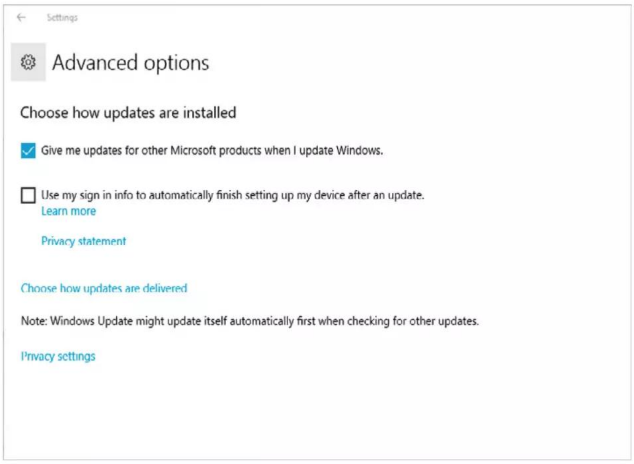
Private (discoverable) network
Firewall is on.
Network is connected.

Public (non-discoverable) network
Firewall is on.
Network is not connected.

Allow an app through the firewall

OFFICE PATCHING

It's not just the Windows core files that require regular updates, if you use Microsoft Office that can be a part of the overall Windows 10 update schedule. There are vulnerabilities in Office too, which when exploited can allow malicious code in the system. Tick the Give me updates for other Microsoft products box in Windows Update's Advanced Options.


Settings

Advanced options

Choose how updates are installed

☑ Give me updates for other Microsoft products when I update Windows.

☐ Use my sign in info to automatically finish setting up my device after an update.
Learn more

Privacy statement

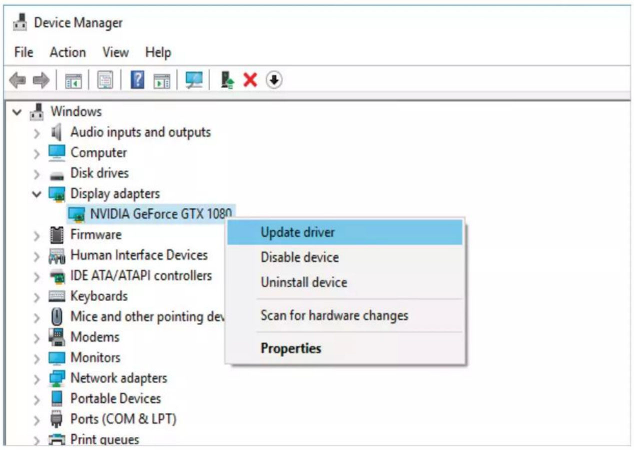
Choose how updates are delivered

Note: Windows Update might update itself automatically first when checking for other updates.

Privacy settings

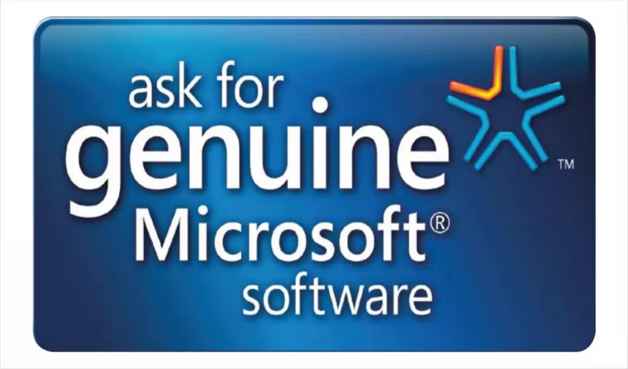
SIGNED DRIVERS

As well as Office, Microsoft provides base-level drivers for most of the hardware available today. These drivers are signed and verified as safe, so any new piece of hardware installed will work and will be safe according to the driver protection engine.


Device Manager
File
Action
View
Help
Windows
Audio inputs and outputs
Computer
Disk drives
Display adapters
NVIDIA GeForce GTX 1080
Firmware
Human Interface Devices
IDE ATA/ATAPI controllers
Keyboards
Mice and other pointing dev
Modems
Monitors
Network adapters
Portable Devices
Ports (COM & LPT)
Print queues
Update driver
Disable device
Uninstall device
Scan for hardware changes
Properties

GENUINE SOFTWARE

Non-genuine copies of Windows have been a thorn in Microsoft's side since illegal file sharing on the Internet gained popularity. These days the act of downloading something illegal is rampant. Windows 10 updates ensure that you're using a genuine copy of the OS, which will ultimately secure you PC against threats from pirated copies.


ask for
genuine
Microsoft®
software
TM

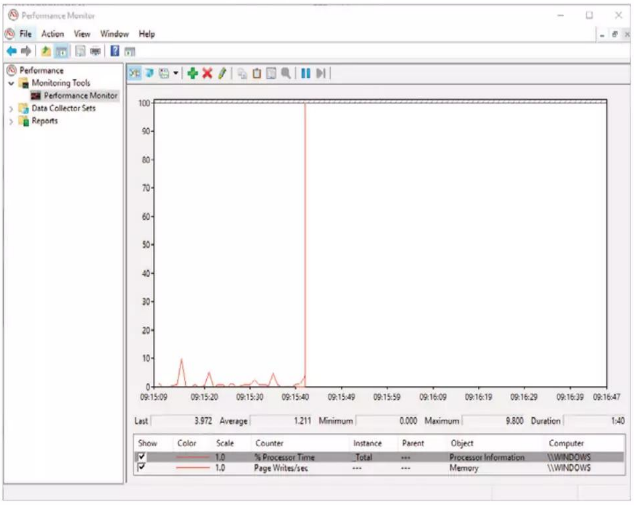
FUTURE UPDATING

Microsoft has big plans for the future of Windows 10, it's often mentioned that this will be the last full version of the OS as they will be running Windows 10 as a service as opposed to different versions over time. This means it will be a constant update cycle with adding or removing of features. Updates ensure you're running the latest versions.

Windows 10
as a Service

STREAMLINING CODE

Updates not only patch any vulnerability, they can also free up system resources by improving the code and streamlining the available resources. In short, if your computer is performing better, then it can easily handle background virus and threat scans without affecting what you're doing.


Performance Monitor
File
Action
View
Window
Help
Performance
Monitoring Tools
Performance Monitor
Data Collector Sets
Reports
100
90
80
70
60
50
40
30
20
10
0
09:15:09
09:15:20
09:15:30
09:15:40
09:15:49
09:15:59
09:16:09
09:16:19
09:16:29
09:16:39
09:16:47

Last 3.972 Average 1.211 Minimum 0.000 Maximum 9.800 Duration 1:40

Show	Color	Scale	Counter	Instance	Parent	Object	Computer
☑		1.0	% Processor Time	_Total	---	Processor Information	\\WINDOWS
☑		1.0	Page Writes/sec	---	---	Memory	\\WINDOWS

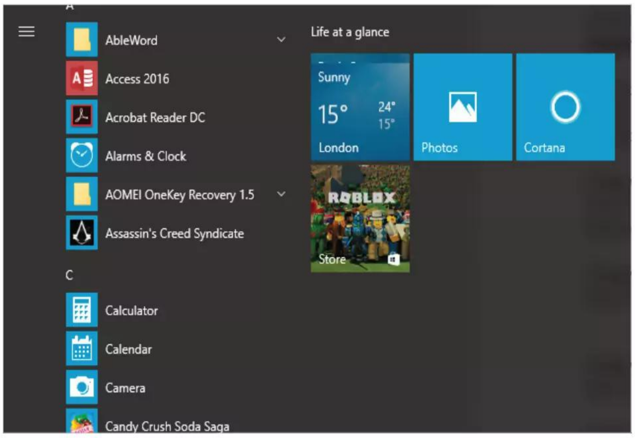
What to Keep Updated and How

Discussing updates is one thing but how do you go about making sure that you have the latest updates and that all the necessary components are being updated correctly? Thanks to the improved update process of Windows 10, this is surprisingly easy.

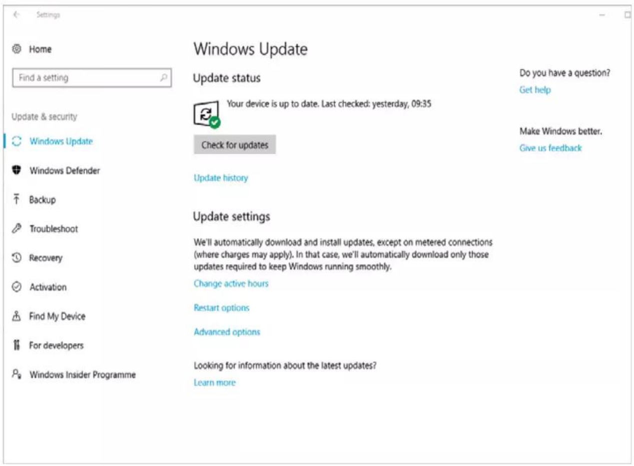
Keeping Up To Date

Whilst it's easy to update Windows 10, there are elements that can be missed. We've already mentioned that it's not only Windows that needs updating but also software and drivers.

STEP 1 The first port of call is undoubtedly Windows Update. Click on the Windows Start button followed by Settings, the cog icon just above the power icon on the strip to the side. This will open the Windows Settings interface, locate the last entry, Update & Security and click it.


AbleWord
Access 2016
Acrobat Reader DC
Alarms & Clock
AOMEI OneKey Recovery 1.5
Assassin's Creed Syndicate
C
Calculator
Calendar
Camera
Candy Crush Soda Saga
Life at a glance
Sunny
15°
24°
15°
London
Photos
Cortana
ROBLOX
Store

STEP 2 By default Windows Update will automatically check for, download and install updates for the core Windows 10 files. You can check for any on the spot by clicking the Check for updates button; and you can see what's already been updated by clicking the Update history link under the update button.


Settings
Home
Find a setting
Update & security
Windows Update
Windows Defender
Backup
Troubleshoot
Recovery
Activation
Find My Device
For developers
Windows Insider Programme
Check for updates
Update history
Change active hours
Restart options
Advanced options
Learn more
Do you have a question?
Get help
Make Windows better.
Give us feedback

Windows Update

Update status

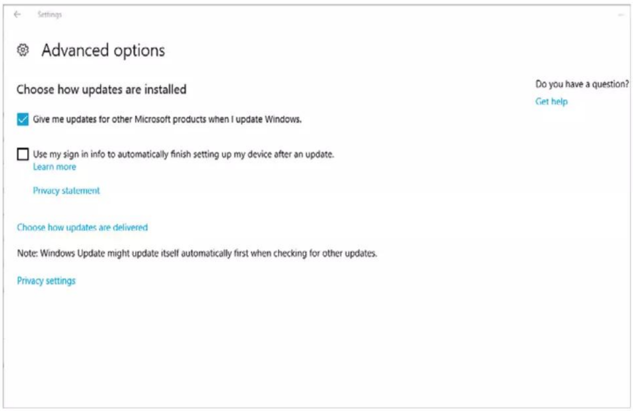
Your device is up to date. Last checked: yesterday, 09:35

Update settings

We'll automatically download and install updates, except on metered connections (where charges may apply). In that case, we'll automatically download only those updates required to keep Windows running smoothly.

Looking for information about the latest updates?

STEP 3 If you click on the Advanced Options link under the Update Settings section, you can then tick a box that enables Windows to automatically check for updates for other Microsoft products, such as Office and so on. It's recommended to make sure the box is ticked, for better security and protection.


Settings
Learn more
Privacy statement
Choose how updates are delivered
Privacy settings
Do you have a question?
Get help

Advanced options

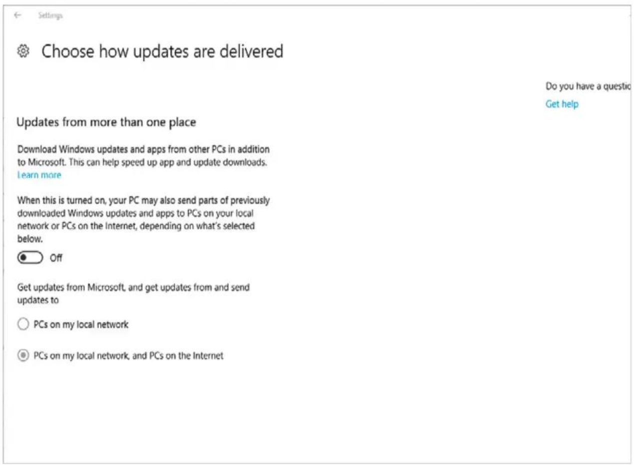
Choose how updates are installed

☑ Give me updates for other Microsoft products when I update Windows.

☐ Use my sign in info to automatically finish setting up my device after an update.

Note: Windows Update might update itself automatically first when checking for other updates.

STEP 4 Within the Advanced Options page click the link for Choose how updates are delivered. This page details the way Windows updates can be pushed to other computers on your network, or even the Internet. Whilst it's a grand idea, there are concerns over privacy from some factors of the community. It's your choice but we prefer this option is Off.


Settings
Learn more
Do you have a questio
Get help

Choose how updates are delivered

Updates from more than one place

Download Windows updates and apps from other PCs in addition to Microsoft. This can help speed up app and update downloads.

When this is turned on, your PC may also send parts of previously downloaded Windows updates and apps to PCs on your local network or PCs on the Internet, depending on what's selected below.

Off

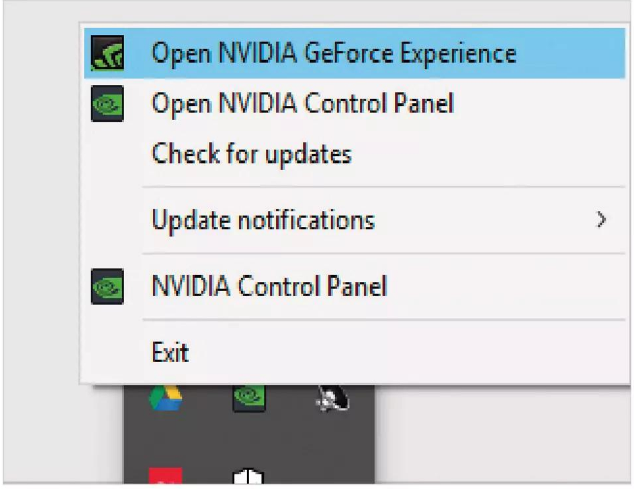
Get updates from Microsoft, and get updates from and send updates to

○ PCs on my local network

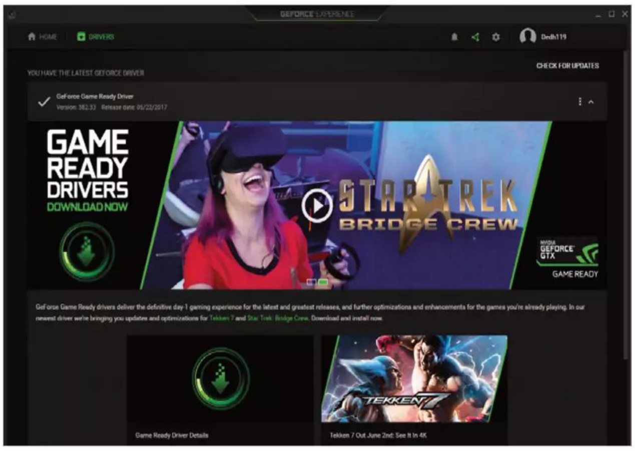
● PCs on my local network, and PCs on the Internet

STEP 5 Hardware drivers are usually automatically updated by Windows Update but whilst signed by Microsoft the drivers themselves aren't always the latest versions. Therein lies a problem: even though signed, the MS drivers won't utilise the hardware as well as the driver developed by the hardware manufacturer.

STEP 6 In such cases it's often best to use the hardware manufacturer's driver, as this is more up to date and features security patches as well as performance updates. For example, if you own an Nvidia graphics card right-click the Nvidia icon in the taskbar and select Open Nvidia GeForce Experience.

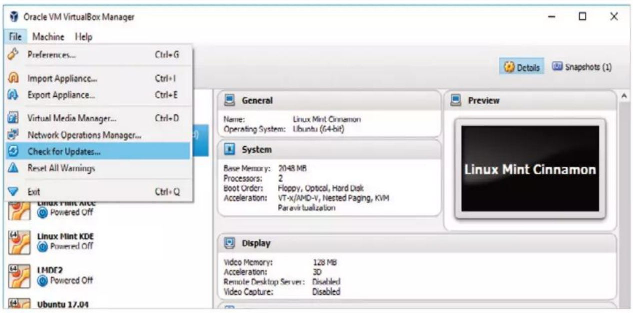

Open NVIDIA GeForce Experience
Open NVIDIA Control Panel
Check for updates
Update notifications
NVIDIA Control Panel
Exit

STEP 7 The Nvidia GeForce Experience allows you to improve in-game graphics and check for the latest drivers. Usually this is done automatically, and you are notified of any available drivers. However, If you want to check manually, click on the Drivers tab followed by Check for Updates.


GEFORCE EXPERIENCE
HOME
DRIVERS
Dedh119
YOU HAVE THE LATEST GEFORCE DRIVER
CHECK FOR UPDATES
GeForce Game Ready Driver
Version: 382.33 Release date: 05/22/2017
GAME READY DRIVERS
DOWNLOAD NOW
STAR TREK
BRIDGE CREW
NVIDIA GEFORCE GTX
GAME READY
TEKKEN 7
Game Ready Driver Details
Tekken 7 Out June 2nd: See It In 4K

GeForce Game Ready drivers deliver the definitive day-1 gaming experience for the latest and greatest releases, and further optimizations and enhancements for the games you're already playing. In our newest driver we're bringing you updates and optimizations for Tekken 7 and Star Trek: Bridge Crew. Download and install now.

STEP 8 Third-party programs and applications also require regular update checks. Again, this is usually done automatically; when you launch the program in question it often checks for the latest version. If not, look for links such as Check for Updates or similar, usually in the Help, About or even under the File menus of your favourite app.

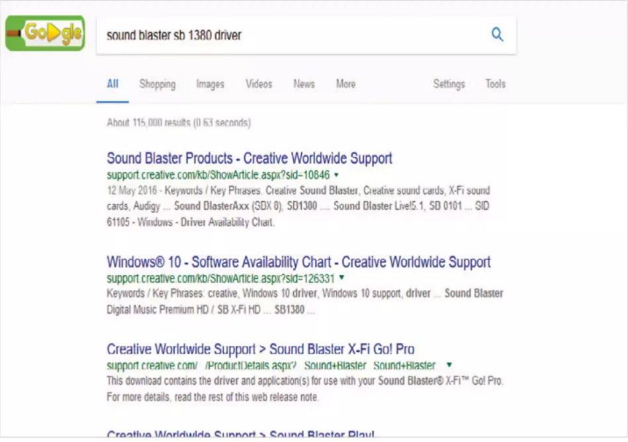

Oracle VM VirtualBox Manager
File
Machine
Help
Preferences... Ctrl+G
Import Appliance... Ctrl+I
Export Appliance... Ctrl+E
Virtual Media Manager... Ctrl+D
Network Operations Manager...
Check for Updates...
Reset All Warnings
Exit Ctrl+Q
Details
Snapshots (1)
General
Preview
System
Display
Linux Mint Cinnamon
Powered Off
Linux Mint KDE
Powered Off
LMDE2
Powered Off
Ubuntu 17.04

Name: Linux Mint Cinnamon
Operating System: Ubuntu (64-bit)

Base Memory: 2048 MB
Processors: 2
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, KVM Paravirtualization

Video Memory: 128 MB
Acceleration: 3D
Remote Desktop Server: Disabled
Video Capture: Disabled

STEP 9 If you've attached some hardware and Windows 10 hasn't been able to load a driver for it, and there isn't any documentation detailing the driver (this often happens with hardware purchased from eBay and the like), then you'll need to hunt one down. Start by locating the device's product name and number and enter it into a search engine.


sound blaster sb 1380 driver
All
Shopping
Images
Videos
News
More
Settings
Tools

About 115,000 results (0.63 seconds)

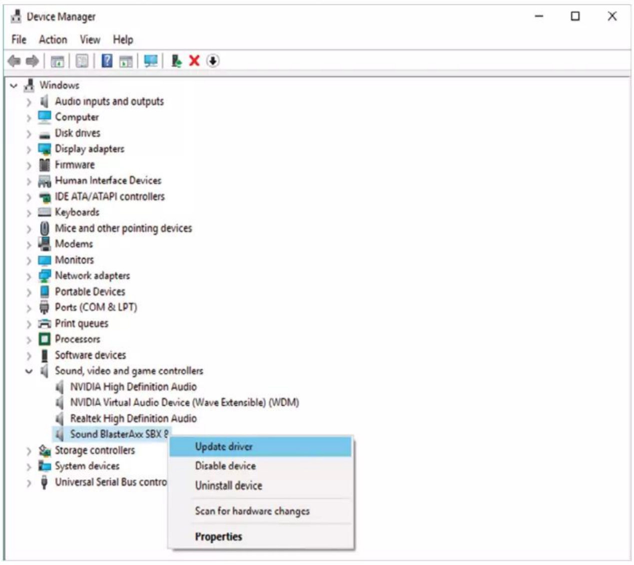
Sound Blaster Products - Creative Worldwide Support
support.creative.com/kb/ShowArticle.aspx?sid=10846
12 May 2016 - Keywords / Key Phrases. Creative Sound Blaster, Creative sound cards, X-Fi sound cards, Audigy ... Sound BlasterAxx (SBX 8), SB1380 .... Sound Blaster Live!5.1, SB 0101 ... SID 61105 - Windows - Driver Availability Chart.

Windows® 10 - Software Availability Chart - Creative Worldwide Support
support.creative.com/kb/ShowArticle.aspx?sid=126331
Keywords / Key Phrases: creative, Windows 10 driver, Windows 10 support, driver ... Sound Blaster Digital Music Premium HD / SB X-Fi HD ... SB1380 ...

Creative Worldwide Support > Sound Blaster X-Fi Go! Pro
support.creative.com/ /ProductDetails.aspx? Sound+Blaster Sound+Blaster
This download contains the driver and application(s) for use with your Sound Blaster® X-Fi™ Go! Pro. For more details, read the rest of this web release note.

Creative Worldwide Support > Sound Blaster Play!

STEP 10 You can often force Windows 10 to locate a driver by right-clicking the Windows Start button and choosing Device Manager from the menu. In the Device Manager window, select the hardware you want updating, right-click it and select Update Driver.


Device Manager
File
Action
View
Help
Windows
Audio inputs and outputs
Computer
Disk drives
Display adapters
Firmware
Human Interface Devices
IDE ATA/ATAPI controllers
Keyboards
Mice and other pointing devices
Modems
Monitors
Network adapters
Portable Devices
Ports (COM & LPT)
Print queues
Processors
Software devices
Sound, video and game controllers
NVIDIA High Definition Audio
NVIDIA Virtual Audio Device (Wave Extensible) (WDM)
Realtek High Definition Audio
Sound BlasterAxx SBX 8
Storage controllers
System devices
Universal Serial Bus contro
Update driver
Disable device
Uninstall device
Scan for hardware changes
Properties

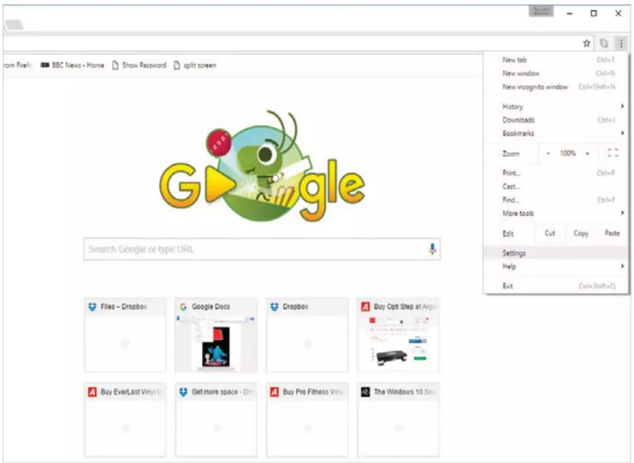
How to Secure Your Web Browser

The web browser is possibly the weakest link in the entire security chain. It's the software product that's on the front line, the one that will inevitably bear the brunt of any Internet attacks and as such, attackers focus a lot of effort on making the browser a portal into your system.

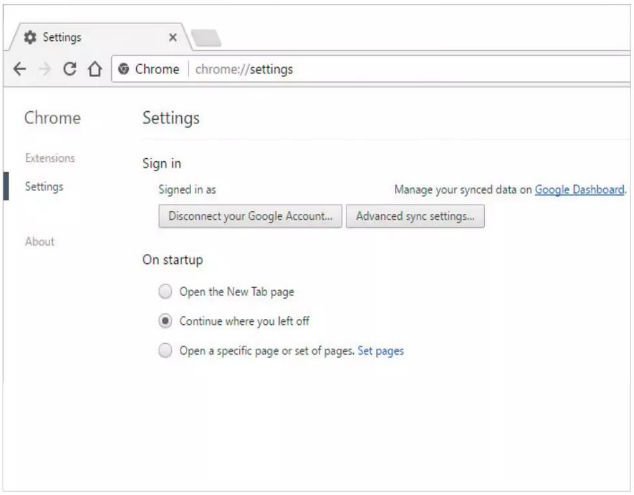
Safer Surfing

Securing your web browser isn't too difficult. There are plenty of options available, including some third-party add-ons you can use to improve security. For this tutorial, we're using Chrome.

STEP 1 Start by opening Chrome and clicking on the three vertical dots in the top right of the browser window. This is the link to the available options; from the list choose Settings.


New tab Ctrl+T
New window Ctrl+N
New incognito window Ctrl+Shift+N
History
Downloads Ctrl+J
Bookmarks
Zoom – 100% +
Print... Ctrl+P
Cast...
Find... Ctrl+F
More tools
Edit Cut Copy Paste
Settings
Help
Exit Ctrl+Shift+Q
Search Google or type URL
Files – Dropbox
Google Docs
Dropbox
Buy Opti Step at App
Buy EverLast Vinyl
Get more space - Dr
Buy Pro Fitness Vin
The Windows 10 Se

STEP 2 It's generally recommended that you sign into Chrome using a Google account, as this can greatly improve the overall security of the browser. For example, when you sign in, under the Sign In section in Settings, click on the Advanced Sync Settings button, the first option available.


Settings
Chrome chrome://settings
Chrome
Extensions
Settings
About

Settings

Sign in

Signed in as

Manage your synced data on Google Dashboard.

Disconnect your Google Account... | Advanced sync settings...

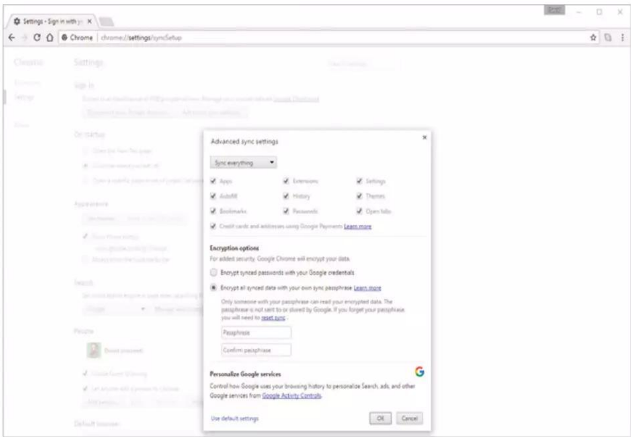
On startup

○ Open the New Tab page

● Continue where you left off

○ Open a specific page or set of pages. Set pages

STEP 3 With the Advanced Sync Settings box open, select the option for Encrypt all synced data with your own sync passphrase. Enter a secure passphrase you can remember in the boxes provided and this will enhance the security of all data synced between Chrome and the Internet.


Settings - Sign in with y
Chrome chrome://settings/syncSetup
Use default settings
OK
Cancel

Advanced sync settings

Sync everything

☑ Apps ☑ Extensions ☑ Settings

☑ Autofill ☑ History ☑ Themes

☑ Bookmarks ☑ Passwords ☑ Open tabs

☑ Credit cards and addresses using Google Payments Learn more

Encryption options

For added security, Google Chrome will encrypt your data.

○ Encrypt synced passwords with your Google credentials

● Encrypt all synced data with your own sync passphrase Learn more

Only someone with your passphrase can read your encrypted data. The passphrase is not sent to or stored by Google. If you forget your passphrase, you will need to reset sync.

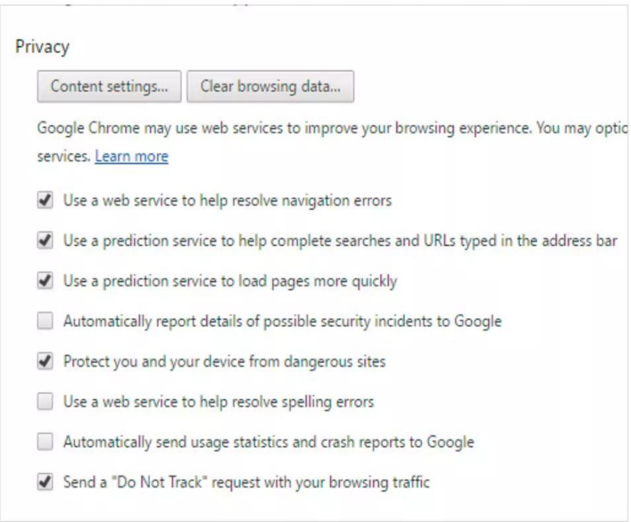
Passphrase

Confirm passphrase

Personalize Google services

Control how Google uses your browsing history to personalize Search, ads, and other Google services from Google Activity Controls.

STEP 4 Look to the bottom of the Settings page and click the link for Show Advanced Settings. The first new section to appear under the Advanced settings is Privacy. Start by clicking on the Content Settings button.


Content settings...
Clear browsing data...

Privacy

Google Chrome may use web services to improve your browsing experience. You may optic services. Learn more

☑ Use a web service to help resolve navigation errors

☑ Use a prediction service to help complete searches and URLs typed in the address bar

☑ Use a prediction service to load pages more quickly

☐ Automatically report details of possible security incidents to Google

☑ Protect you and your device from dangerous sites

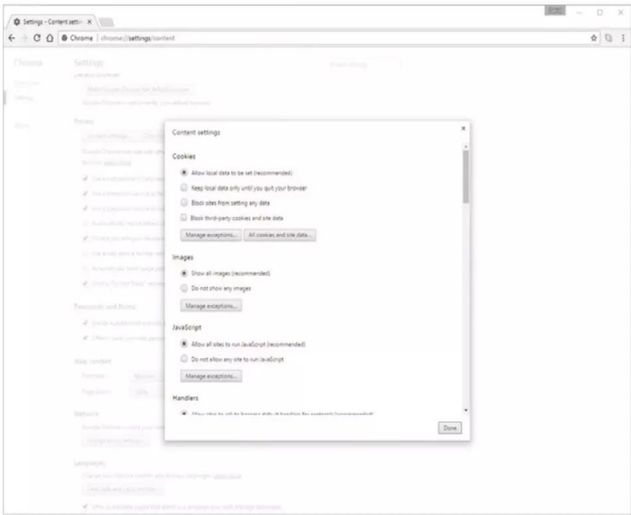
☐ Use a web service to help resolve spelling errors

☐ Automatically send usage statistics and crash reports to Google

☑ Send a "Do Not Track" request with your browsing traffic

STEP 5

Content Settings allows a greater degree of control over Cookies, JavaScript, Flash, Pop-ups, your computer's microphone and even the webcam. It's an extensive list so we can't go into all the options within this limited space. For maximum security, disable JavaScript and Flash and make sure the mic and webcam are protected too.



Content settings

Cookies

● Allow local data to be set (recommended)
○ Keep local data only until you quit your browser
○ Block sites from setting any data
☐ Block third-party cookies and site data

Images

● Show all images (recommended)
○ Do not show any images

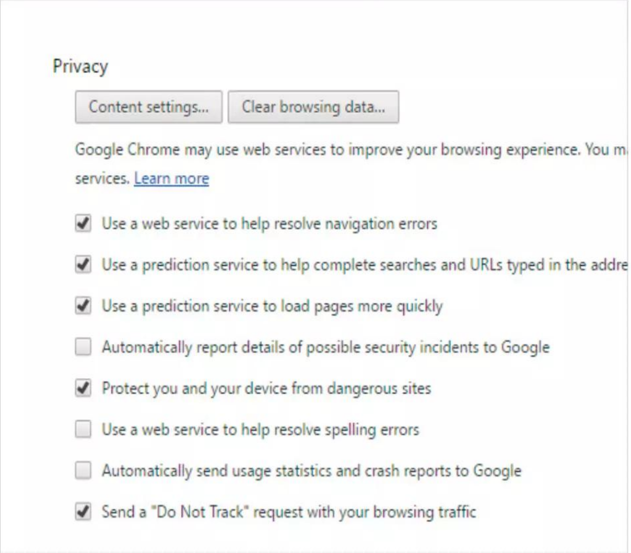
JavaScript

● Allow all sites to run JavaScript (recommended)
○ Do not allow any site to run JavaScript

Handlers

STEP 6

Click the Done button when you're finished with Content Settings, to return you to the Chrome Settings page. Within Privacy still, ensure the last option, Send a "Do Not Track" request, is ticked. This will stop any tracking elements from monitoring your browsing activities.



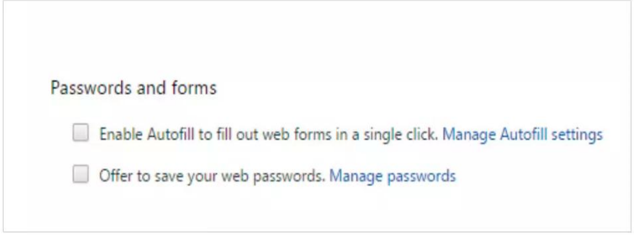
Privacy

Google Chrome may use web services to improve your browsing experience. You m
services. Learn more

☑ Use a web service to help resolve navigation errors
☑ Use a prediction service to help complete searches and URLs typed in the addre
☑ Use a prediction service to load pages more quickly
☐ Automatically report details of possible security incidents to Google
☑ Protect you and your device from dangerous sites
☐ Use a web service to help resolve spelling errors
☐ Automatically send usage statistics and crash reports to Google
☑ Send a "Do Not Track" request with your browsing traffic

STEP 7

Just under the previous step's tick box, it's also recommended to untick the two Passwords and Forms boxes that offer to enable Autofill and Save your Passwords. Whilst it's a pain to constantly enter passwords, this will stop any hijack Chrome attacks from gaining your usernames and passwords.

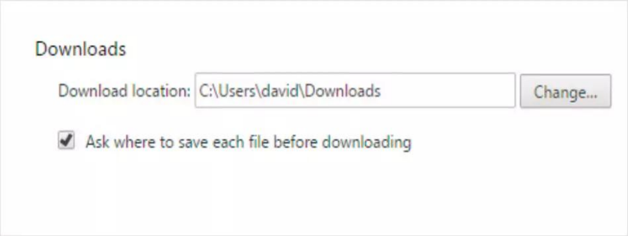


Passwords and forms

☐ Enable Autofill to fill out web forms in a single click. Manage Autofill settings
☐ Offer to save your web passwords. Manage passwords

STEP 8

Under the Downloads section, it's an idea to tick the box Ask where to save each file before downloading. Again this can be a bit of a pain for the user; however it stops malicious background downloads from infecting your system, giving you more control and the ability to stop the process.



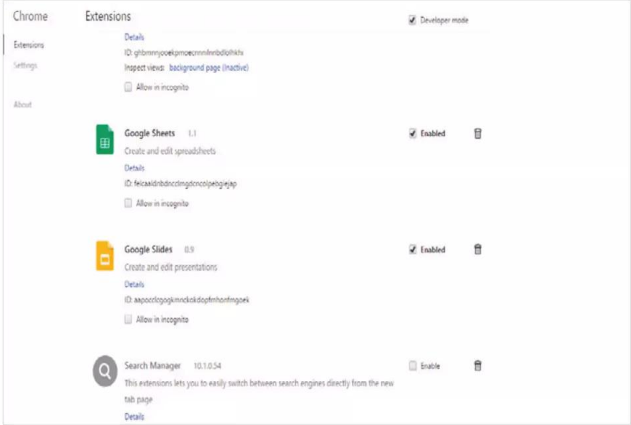
Downloads

Download location: C:\Users\david\Downloads

☑ Ask where to save each file before downloading

STEP 9

To the left of the Chrome Settings page you can see links for Extensions, Settings and About; click the Extensions link. With the Extensions page open, scroll down to the bottom and click the Get More Extensions link.



☑ Developer mode

Details
ID: ghbmnnjooekpmoecnnnilnnbdlolhkhi
Inspect views: background page (Inactive)
☐ Allow in incognito

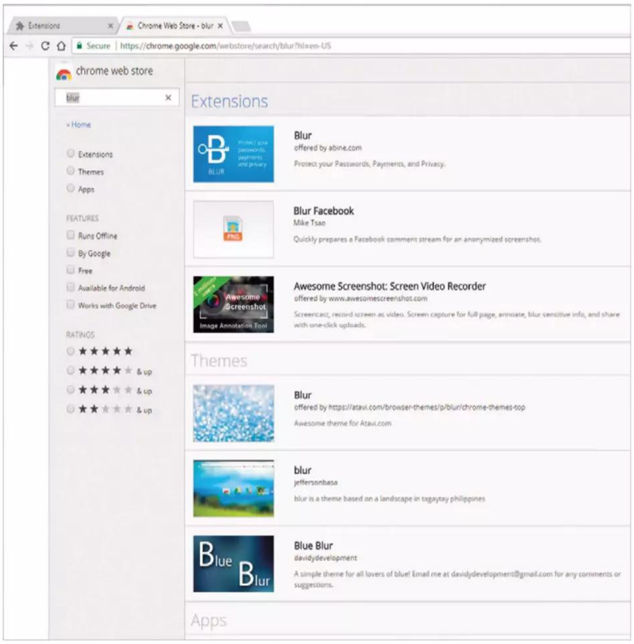
Google Sheets 1.1 ☑ Enabled
Create and edit spreadsheets
Details
ID: felcaaldnbdncclmgdcncolpebgiejap
☐ Allow in incognito

Google Slides 0.9 ☑ Enabled
Create and edit presentations
Details
ID: aapocclcgogkmnckokdopfmhonfmgoek
☐ Allow in incognito

Search Manager 10.1.0.54 ☐ Enable
This extensions lets you to easily switch between search engines directly from the new tab page
Details

STEP 10

With the Chrome Web Store launched, via the Extensions link, search for Adblock Plus. Within the results, click on the Add to Chrome button on first option for Adblock Plus. This will install an advertising blocker within Chrome, securing you from any threats from Internet advertising. Do the same for Blur (an anti-tracking add-on) and HTTPS Everywhere.



Secure | https://chrome.google.com/webstore/search/blur?hl=en-US

Blur
offered by abine.com
Protect your Passwords, Payments, and Privacy.

Blur Facebook
Mike Tsao
Quickly prepares a Facebook comment stream for an anonymized screenshot.

Awesome Screenshot: Screen Video Recorder
offered by www.awesomescreenshot.com
Screencast, record screen as video. Screen capture for full page, annotate, blur sensitive info, and share with one-click uploads.

Blur
offered by https://atavi.com/browser-themes/p/blur/chrome-themes-top
Awesome theme for Atavi.com

blur
jeffersonbasa
blur is a theme based on a landscape in tagaytay philippines

Blue Blur
davidydevelopment
A simple theme for all lovers of blue! Email me at davidydevelopment@gmail.com for any comments or suggestions.

How to Secure Your Home Network

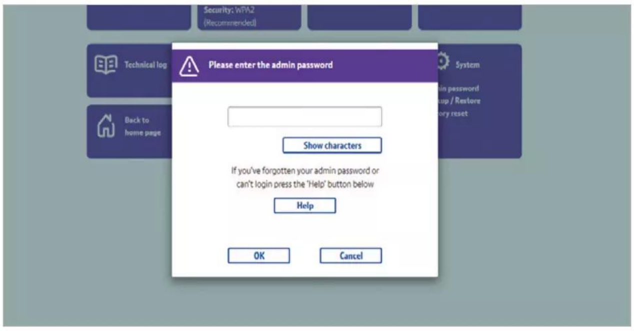
We've mentioned previously that an attack doesn't always come from the other side of the globe but can indeed be a little too close to home at times. Home network hacking is possible with the simplest of tools available on the Internet, often even just tapping into a cable.

Network Protection

Without being too paranoid, it's remarkably easy to get into a neighbour's home network. If you live in a block of flats or you use powerline adapters, you may need to consider these ten steps for better network protection.

ROUTER PASSWORD

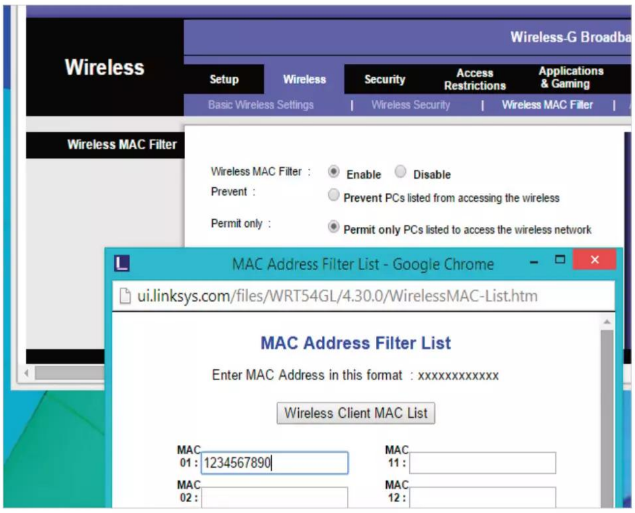
The most common entry point to gain access to your network is via the router. The router from your ISP may well be offering the latest forms of encryption but it doesn't take a genius to trawl the less reputable sections of the Internet to obtain a list of passwords. Therefore, change the default username and password to access it.


Security: WPA2
(Recommended)
Technical log
Back to
home page
System
Please enter the admin password
Show characters
Help
OK
Cancel

If you've forgotten your admin password or can't login press the 'Help' button below

MAC ADDRESSING

Most routers these days come with a form of authentication called MAC (Media Access Code) address filtering. Every networkable device, computers, tablets, games consoles, come with a unique MAC address. The filtering allows you to enter the MAC addresses of your devices, so only they can be used on your router. Consult your router documentation for more details.


Wireless
Wireless-G Broadba
Setup
Wireless
Security
Access
Restrictions
Applications
& Gaming
Basic Wireless Settings
Wireless Security
Wireless MAC Filter
Wireless MAC Filter
MAC Address Filter List - Google Chrome
MAC Address Filter List
Wireless Client MAC List

Wireless MAC Filter : ● Enable ○ Disable

Prevent : ○ Prevent PCs listed from accessing the wireless

Permit only : ● Permit only PCs listed to access the wireless network

ui.linksys.com/files/WRT54GL/4.30.0/WirelessMAC-List.htm

Enter MAC Address in this format : xxxxxxxxxxxx

MAC 01 : 1234567890

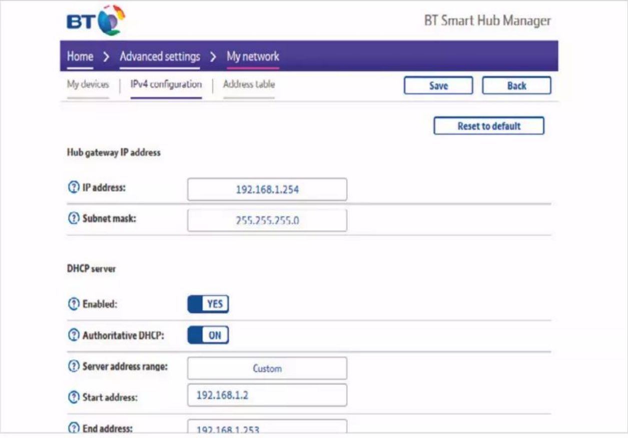
MAC 02 :

MAC 11 :

MAC 12 :

DISABLE DHCP

It can be a pain but try disabling DHCP on your router and opting for static IP addresses. Every device that connects to a DHCP router will receive an IP address. By eliminating that you get to specify the address range available. It's not fool proof but it's worth considering.


BT
BT Smart Hub Manager
Home
Advanced settings
My network
My devices
IPv4 configuration
Address table
Save
Back
Reset to default

Hub gateway IP address

IP address: 192.168.1.254

Subnet mask: 255.255.255.0

DHCP server

Enabled: YES

Authoritative DHCP: ON

Server address range: Custom

Start address: 192.168.1.2

End address: 192.168.1.253

POWER OFF

According to Trustwave's 2013 Global Security Report, many home network hacks are conducted when the household is away or asleep. This leaves the hacker with ample opportunity to steal bandwidth and view files you may have on a NAS drive. The short, simple solution is to power off the router at night and if you go out for the day.

POWERLINE ENCRYPTION

Powerline adapters are an excellent resource for connecting wired network devices, without trailing lengths of cable around the home. However, depending on the adapter, it is possible to use another adapter to gain access to yours. Newer homes are common where you're able to pick up another network, so use the encryption button if the adapter has one.

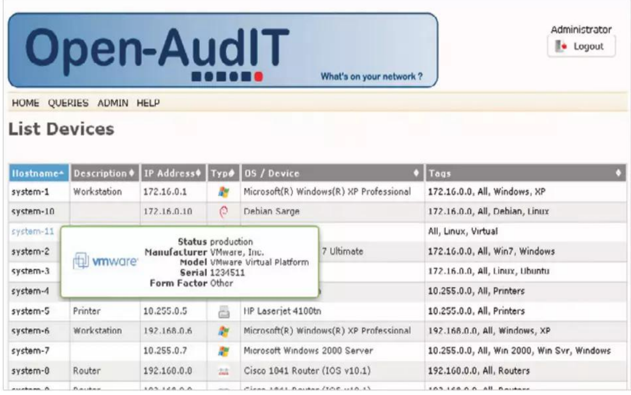
devolo
500Mbps

ETHERNET CABLES

Cabling a home with Ethernet isn't a difficult project, this offers faster connection speeds than that of wireless; but if you're living in shared accomodation or a flat block, make sure that any unseen cable lengths can't be access by a neighbour. It's easy enough to splice into an Ethernet cable and steal bandwidth.

NETWORK MAPPING

Consider using a network mapping program, such as Open-AudIT, to gain a better understanding of what devices are attached to your network. Become familiar with the addresses, manufacturer, model IDs and so on of every connected object. That way, should anything new appear, you'll know it's not something you allowed.



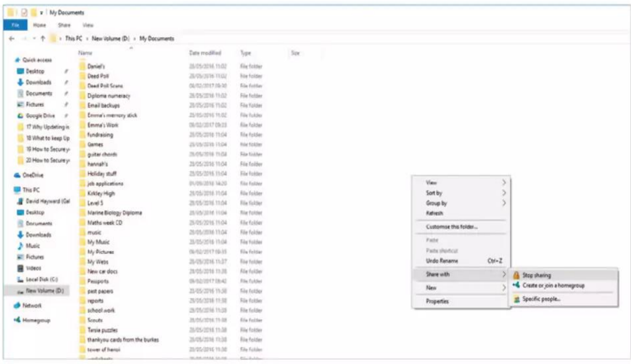
List Devices

Hostname	Description	IP Address	Type	OS / Device	Tags
system-1	Workstation	172.16.0.1		Microsoft(R) Windows(R) XP Professional	172.16.0.0, All, Windows, XP
system-10		172.16.0.10		Debian Sarge	172.16.0.0, All, Debian, Linux
system-11					All, Linux, Virtual
system-2				7 Ultimate	172.16.0.0, All, Win7, Windows
system-3					172.16.0.0, All, Linux, Ubuntu
system-4					10.255.0.0, All, Printers
system-5	Printer	10.255.0.5		HP Laserjet 4100tn	10.255.0.0, All, Printers
system-6	Workstation	192.168.0.6		Microsoft(R) Windows(R) XP Professional	192.168.0.0, All, Windows, XP
system-7		10.255.0.7		Microsoft Windows 2000 Server	10.255.0.0, All, Win 2000, Win Svr, Windows
system-8	Router	192.168.0.8		Cisco 1041 Router (IOS v10.1)	192.168.0.0, All, Routers

vmware
Status production
Manufacturer VMware, Inc.
Model VMware Virtual Platform
Serial 1234511
Form Factor Other

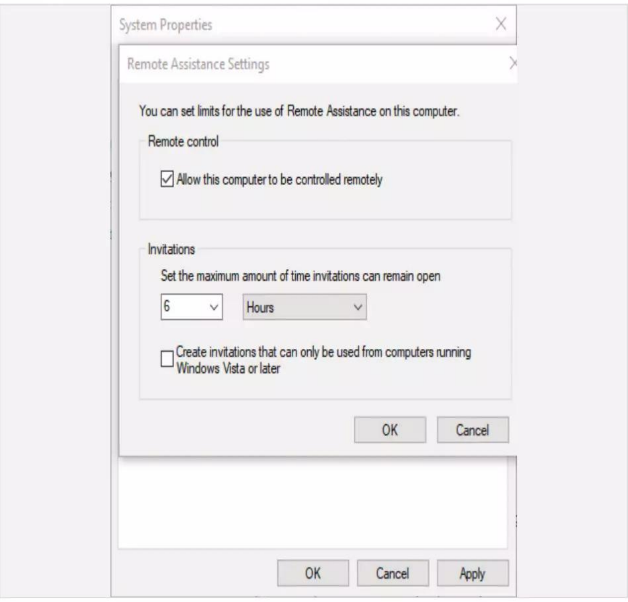
SHARE LESS

Sharing resources and files from one computer to another is perfectly fine but consider sharing less if you live in close proximity to others. Once a hacker has gained access to your network, getting to any shared folders you have will be a doddle. In extreme cases don't share anything but generally tighten password control.



REMOTE ACCESS

Remote administration on both the router and computer certainly help you out when you're not at the keyboard. Perhaps you connect to your home network from work? Whatever the reasons, it does leave a potential gap in your home network security. Consider closing it completely or double-checking the authentication is top notch.



You can set limits for the use of Remote Assistance on this computer.

Remote control

☑ Allow this computer to be controlled remotely

Invitations

Set the maximum amount of time invitations can remain open

6 Hours

☐ Create invitations that can only be used from computers running Windows Vista or later

VISIBLE PORTS

If you run a small office make sure that all your wall ports are located in areas where they are secure. Behind desks and generally away from where the public or any visitors may be able sneakily plug a laptop in.

What are Wireless Security Standards?

Wireless security has adhered to a number of standards since 1999, each improving over the last due to the ability for a then-modern computer to hack the security levels behind them. Tighter controls are needed as computers and the way they connect have become increasingly more complex.

WEP, WPA, WPA2, IEEE…

Amid the confusing acronyms lies a logical progression of wireless encryption and security protocols. Whilst at first they seem bewildering, it's quite interesting to learn of their history.

The technology behind delivering a wireless network has evolved over the last couple of decades and so has the ways and means in which to secure it all. It's not just simply down to choosing a password that no one is likely to guess, you need to make sure that data and connection to a wireless network is encrypted to the highest possible standard.

These standards are always moving forward and like most elements of the technology industry they come with a bewildering cocktail of acronyms and meanings. Encryption and all things security can be a confusing topic, even for experts. Here are the current, and most important, terms you should be familiar with when talking about wireless security standards, wireless networking and the hardware that lies between your wireless communications.

IEEE

The Institute of Electrical and Electronics Engineers is the organisation responsible for setting the entire wireless security industry, and data communications standards. It was founded, surprisingly, back in 1963 and is regarded as the largest association of technical professionals in the world.

IEEE 802.11
b
g
a
n

802.1x

You've no doubt come across the numbers 802.11 when looking at wireless-based and networking documentation but what on earth does it mean? 802.1x is the IEEE standard for providing authentication and controlling user traffic across wireless and wired Ethernet-based networks. It's an ideal application for providing authentication for wireless networks, as it requires very little processing power from the authenticator: the actual wireless access point. The better the standard, ending with a, b, g, n, ac and so on, the higher the speed of communications between devices.

WPA2

WPA2 is the upgraded standard security technology of WPA. It's designed to offer the user an impressive 256-bit encryption key, which is virtually uncrackable unless you're a secret research lab with a few billion dollars to spare on quantum computing and dedicated hardware decrypting processors. There are also different sub-standards within WPA2, with AES (Advanced Encryption Standard) and TKIP (Temporal Key Integrity Protocol), both of which are encryption methods, along with the lesser used CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol).

WEP

This is the original wireless encryption security standard, Wired Equivalent Privacy. Whilst the protocol worked for the late nineties wireless networks, it was soon overshadowed by the ever increasing power of the average computer. WEP uses a 40-bit standard encryption key, which is a key consisting of either 10 or 26 hexadecimal digits. That sounds like a lot of possible keys to crack but a modern, powerful computer would be able to break 40-bit encryption in around 30 seconds; compare this to months for a computer in the late '90s.

Access Point

Talking about access points, this is the hardware that acts as a receiver or transmitter for the wireless signal and network. It can physically be a number of different components, such as a router, switch or powerline adapter but essentially it's the hardware that converts a wired Ethernet network to a 2.4GHz or 5GHz wireless signal and vice versa; it's also referred as the WAP, Wireless Access Point.

WPA

Replacing the WEP standard, WPA (Wi-Fi Protected Access) provided a much needed improvement for the ever advancing march of security. It became the standard in 2003 and offered the user either 64-bit or the more adept 128-bit key levels of encryption. A 64-bit key attack would take several lifetimes when it was first introduced; these days it's estimated that it would take several months, maybe less if the attacker used several computers working as a cluster. Naturally 128-bit key lengths are mind-numbingly more complex and even by today's standards, the theoretical process of a brute force attack would take more time than the universe has estimated left to exist. Which is a very, very long time.

How to Secure Your Wireless Network

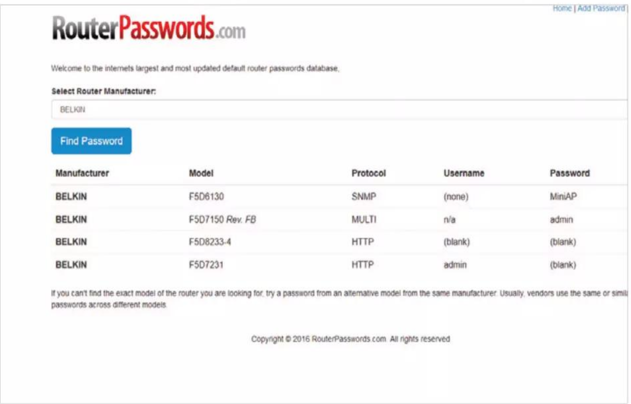
It may seem a little far-fetched but it's not unfeasible for a hacker to sit outside your house with a tablet or laptop and gain access to your home network via the router's Wi-Fi signal. Understandably it's quite rare but it's worth considering beefing up your protection.

Wi-Fi, Lock and Key

A lot of the standard tips on protecting your Wi-Fi merge with those of protecting your wired network. It's common sense mostly and keeping an eye on what's going on in your own network.

ADMIN PASSWORD

All routers come with a generic username and password. Depending on the model and manufacturer of the router, it's surprisingly easy to get hold of the username and password. For example, view www.routerpasswords.com and choose your router. With that being the case, change the administrator username and its password.


Home | Add Password
RouterPasswords.com
Find Password

Welcome to the internets largest and most updated default router passwords database.

Select Router Manufacturer: BELKIN

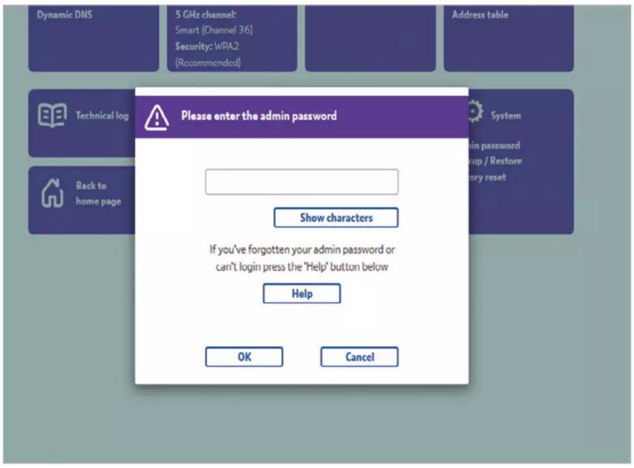
Manufacturer	Model	Protocol	Username	Password
BELKIN	F5D6130	SNMP	(none)	MiniAP
BELKIN	F5D7150 *Rev. FB*	MULTI	n/a	admin
BELKIN	F5D8233-4	HTTP	(blank)	(blank)
BELKIN	F5D7231	HTTP	admin	(blank)

If you can't find the exact model of the router you are looking for, try a password from an alternative model from the same manufacturer. Usually, vendors use the same or simi passwords across different models.

Copyright © 2016 RouterPasswords.com. All rights reserved.

ISP PASSWORD

ISP supplied routers tend to have their own set of usernames and passwords. Although these are more secure than that of the default set, they are still obtainable from the more dubious quarter of the Internet. A potential hacker will easily be able to get hold of sets of passwords, so where possible change the ISP default username and password.


Dynamic DNS
Address table
Technical log
Back to home page
System
in password
up / Restore
ory reset
Show characters
Help
OK
Cancel

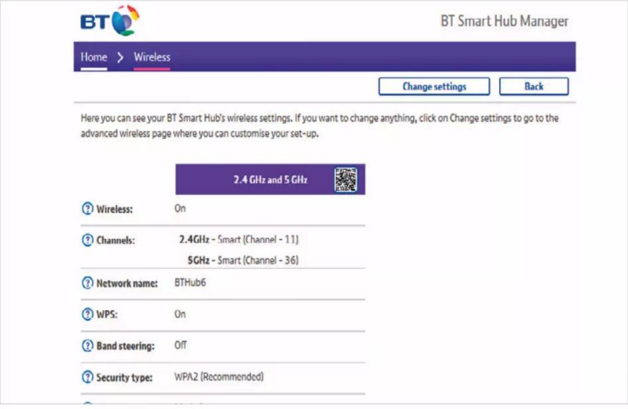
5 GHz channel: Smart (Channel 36)
Security: WPA2 (Recommended)

Please enter the admin password

If you've forgotten your admin password or can't login press the 'Help' button below

CHANGE SSID

The Service Set Identifier (SSID) is the name of the router that's broadcast so you're able to locate and connect to it. Most routers will display the name and ISP, or the make and model, making it easier for a hacker to find the information they need to gain access. It's recommend therefore to frequently change the SSID.

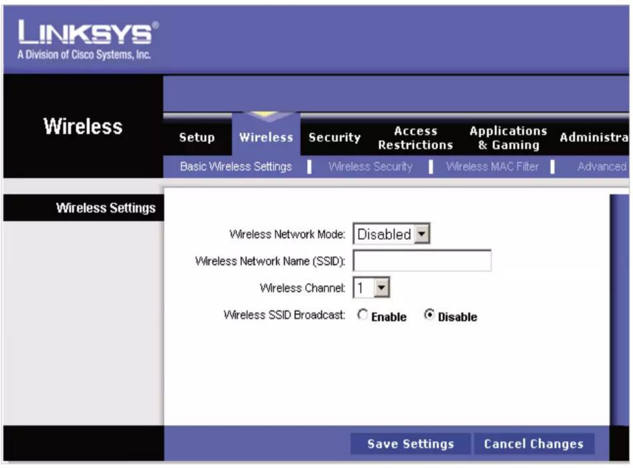

BT
BT Smart Hub Manager
Home > Wireless
Change settings
Back
2.4 GHz and 5 GHz

Here you can see your BT Smart Hub's wireless settings. If you want to change anything, click on Change settings to go to the advanced wireless page where you can customise your set-up.

Wireless: On
Channels: 2.4GHz - Smart (Channel - 11)
5GHz - Smart (Channel - 36)
Network name: BTHub6
WPS: On
Band steering: Off
Security type: WPA2 (Recommended)

HIDE SSID

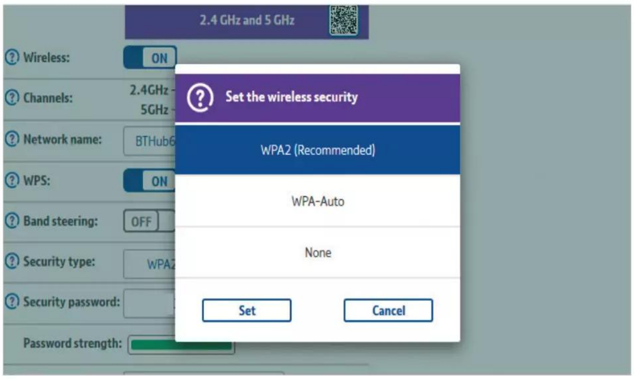
It's also possible to select an option to hide your SSID from being broadcast. Whilst this doesn't stop it being hacked, it does make it a little more difficult for someone who's casually looking around for networks to access. You'll need to consult your router documentation to find how to hide your SSID for make and model.


LINKSYS®
A Division of Cisco Systems, Inc.
Wireless
Setup
Wireless
Security
Access Restrictions
Applications & Gaming
Administra
Basic Wireless Settings
Wireless Security
Wireless MAC Filter
Advanced
Wireless Settings
Save Settings
Cancel Changes

Wireless Network Mode: Disabled
Wireless Network Name (SSID):
Wireless Channel: 1
Wireless SSID Broadcast: ○ Enable ● Disable

USE WPA2

Most modern routers will already come with the latest security standard enabled, WPA2; but there are instances of some routers defaulting to a lesser security type for the sake of device compatibility. It's essential that you ensure your router is using the latest and best form of encryption for your protection.



2.4 GHz and 5 GHz

Wireless: ON

Channels: 2.4GHz
5GHz

Network name: BTHub6

WPS: ON

Band steering: OFF

Security type: WPA2

Security password:

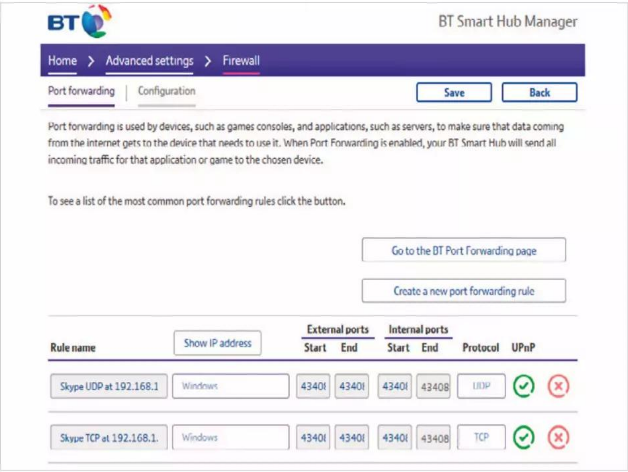
Password strength:

Set the wireless security

- WPA2 (Recommended)
- WPA-Auto
- None

ROUTER FIREWALL

The firewall that comes with Windows 10 is good but the firewall from third-party AV software is even better; and for extra protection, make sure that the router's firewall is enabled and doesn't have any potential leaks.



BT Smart Hub Manager

Home > Advanced settings > Firewall

Port forwarding | Configuration

Port forwarding is used by devices, such as games consoles, and applications, such as servers, to make sure that data coming from the internet gets to the device that needs to use it. When Port Forwarding is enabled, your BT Smart Hub will send all incoming traffic for that application or game to the chosen device.

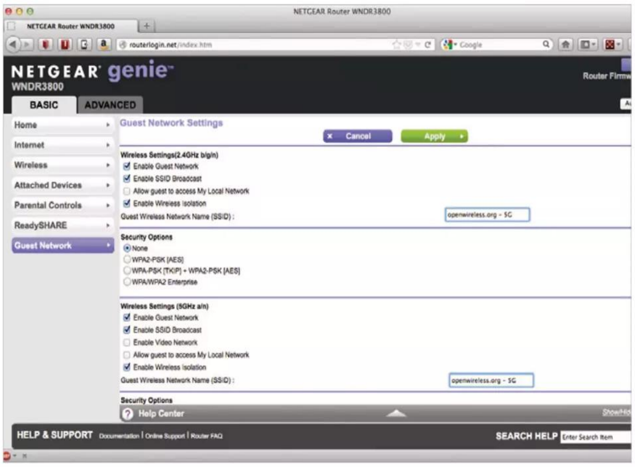
To see a list of the most common port forwarding rules click the button.

Go to the BT Port Forwarding page
Create a new port forwarding rule

Rule name	Show IP address	External ports Start	External ports End	Internal ports Start	Internal ports End	Protocol	UPnP	
Skype UDP at 192.168.1	Windows	4340(	4340(	4340(	43408	UDP	✓	⊗
Skype TCP at 192.168.1.	Windows	4340(	4340(	4340(	43408	TCP	✓	⊗

DISABLE GUEST

Some routers come equipped with the ability to allow a guest network. This enables users to connect to the router without requiring an encrypted password. Obviously this is a potential huge gap in your home network security. If you have no need of a guest network, then look to the documentation on how to disable it.



NETGEAR Router WNDR3800
routerlogin.net/index.htm
NETGEAR genie
WNDR3800
BASIC
ADVANCED
Home
Internet
Wireless
Attached Devices
Parental Controls
ReadySHARE
Guest Network
Cancel
Apply

Guest Network Settings

Wireless Settings(2.4GHz b/g/n)
- ☑ Enable Guest Network
- ☑ Enable SSID Broadcast
- ☐ Allow guest to access My Local Network
- ☑ Enable Wireless Isolation

Guest Wireless Network Name (SSID) : openwireless.org - 5G

Security Options
- ● None
- ○ WPA2-PSK [AES]
- ○ WPA-PSK [TKIP] + WPA2-PSK [AES]
- ○ WPA/WPA2 Enterprise

Wireless Settings (5GHz a/n)
- ☑ Enable Guest Network
- ☑ Enable SSID Broadcast
- ☐ Enable Video Network
- ☐ Allow guest to access My Local Network
- ☑ Enable Wireless Isolation

Guest Wireless Network Name (SSID) : openwireless.org - 5G

Security Options

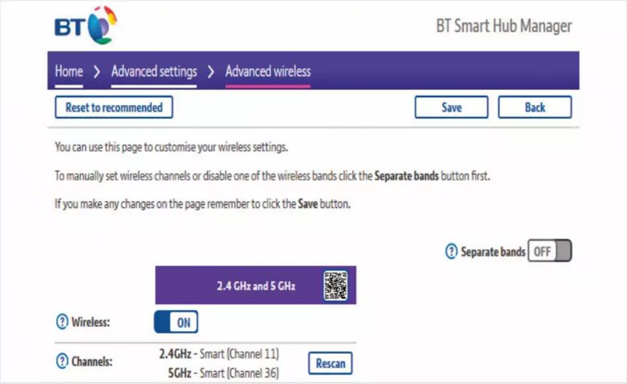
Help Center
HELP & SUPPORT Documentation | Online Support | Router FAQ
SEARCH HELP Enter Search Item

ROUTER RELOCATION

Most users will have their router located in the living room, near the master phone socket. This means that not only will the router broadcast through the house, it's also broadcasting over much of the street in front. Consider placing the router in a more central location of your house. This offers great coverage, whilst limiting its signal reach beyond.

DISABLE WPS

The WPS button on a router and a device will allow easy pairing of the two without the need to enter the encryption password. This is certainly convenient but someone who may gain physical access to your router will be able to pair their own device. Look to turning off WPS in the router's settings.



BT Smart Hub Manager

Home > Advanced settings > Advanced wireless

Reset to recommended
Save
Back

You can use this page to customise your wireless settings.

To manually set wireless channels or disable one of the wireless bands click the **Separate bands** button first.

If you make any changes on the page remember to click the **Save** button.

Separate bands: OFF

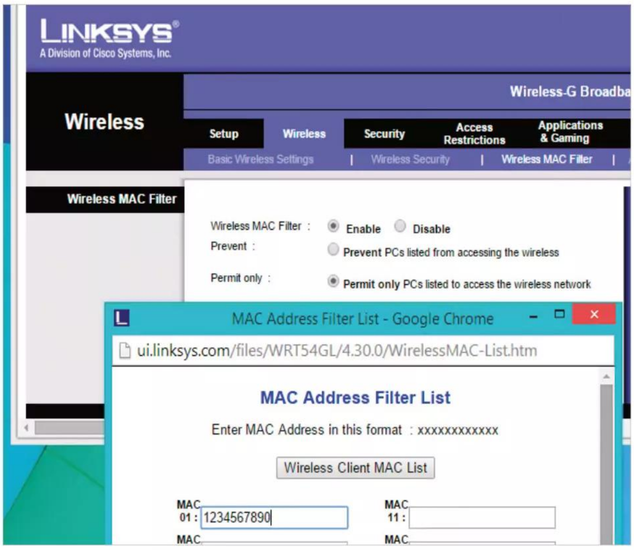
2.4 GHz and 5 GHz

Wireless: ON

Channels: 2.4GHz - Smart (Channel 11)
5GHz - Smart (Channel 36)

MAC FILTERING

Filtering MAC addresses was discussed previously but it's worth repeating with regards to wireless network security. By filtering those devices that are allowed to connect to your router, and keeping an eye on what's connecting, you're able to control your security to a far higher degree than usual.



LINKSYS
A Division of Cisco Systems, Inc.
Wireless-G Broadba
Wireless
Setup
Wireless
Security
Access Restrictions
Applications & Gaming
Basic Wireless Settings
Wireless Security
Wireless MAC Filter
Wireless MAC Filter

Wireless MAC Filter : ● Enable ○ Disable

Prevent : ○ Prevent PCs listed from accessing the wireless

Permit only : ● Permit only PCs listed to access the wireless network

MAC Address Filter List - Google Chrome

ui.linksys.com/files/WRT54GL/4.30.0/WirelessMAC-List.htm

MAC Address Filter List

Enter MAC Address in this format : xxxxxxxxxxxx

Wireless Client MAC List

MAC 01 : 1234567890

MAC 11 :

What is Encryption?

We've mentioned encryption and its impact on your privacy and security, but what exactly is it? The definition of encryption is 'the process of converting information or data into a code, to prevent unauthorised access'.

Kryptos Communications

To better understand encryption it's worth taking a moment to learn about its origins, how it's been developed over the years and how it applies to our modern communications.

The word encryption comes from the ancient Greek word Kryptos, which means hidden or secret. Interestingly, the use of hiding messages from others can be traced back to early Egyptian scribes who inserted non-standard hieroglyphs within other communications in order to hide the message from casual viewers. According to historians the Spartans used strips of leather with messages engraved. When the strips were read they were meaningless but when wrapped around a staff of a certain diameter the characters would be decipherable.

Of course, the modern forms of encryption are far more advanced but the overall core concept has remained the same: to be able to send a message to others without anyone else being able to decipher it. However, modern encryption now requires more than simply sending coded messages. Not only is confidentiality required, encryption must perform a level of authentication, so the origin of the communication can be verified; integrity of the communications, where both the sender and those who receive the communication can be ensured that the message hasn't been altered in between; and some form of nonrepudiation, where the sender cannot deny having sent the communication in the first place.

During the early digital age the only users of encryption were the government and military, and as such between them they created a set of algorithms and standards to protect the communication on the battlefield and from one government agency to the next. These algorithms grew in complexity as technology advanced and it wasn't long before the military-based forms of encryption were being used in commercial modes of communications. Within a few short years, bank transfers, cash withdrawals and data sent to and from modems began utilising these new protocols to protect sensitive information.

Today we're regularly seeing and using devices that boast 'military grade 256-bit AES' forms of encryption, a standard that is regarded as nearly impossible to break without spending billions on specialist hardware and software. In plain English, the modern form of encryption takes data and passes it through an algorithm together with a key. This creates a garbled file of characters that can only be clearly read if the correct key is applied to decrypt the data. Algorithms today are divided into two categories: symmetric and asymmetric.

Symmetric key ciphers use the same key to both encrypt and decrypt data. The most popular symmetric cipher is AES (Advanced Encryption Standard), developed by the military and government to protect communications and data. This is a fast form of decryption that requires the sender to exchange the key used to encrypt the data with the recipient before they're able to read it.

Asymmetric key ciphers are also known as public-key cryptography and utilise two mathematically linked keys, public and private. The public key can be shared with everyone and is usually generated by software or provided by a designated authority. The private key is something that's usually only known by the individual user. Interestingly both types of keys can be applied, where one user has a public key and another a private key, which can be combined to form a shared encryption level.

These keys are many characters in length, proving it nigh impossible for someone to Brute Force hack them. The Brute Force method involves using a program on a computer to try every possible combination of a key until the correct one is found. In the case of the 256-bit encryption, it would take 2^{256} different combinations to break the key. If you were able to force one trillion keys per second, it would still take you somewhere in the region of 10^{57} years in order to crack 256-bit encryption. However, a powerful computer can probably manage around two billion calculations per second, so in theory it would take 9.2^{50} years for your standard desktop to crack it. Take in mind that the universe has theoretically only been in existence for 1.4^{10} years.

Numbers as big as that are generally far too mind-boggling to comprehend. Suffice to say that if you're able to use 256-bit encryption for your communications or to protect your data, then you're going to be protected for at least seven times the current age of the universe.

> *Encryption is the act of protecting your data from prying eyes*

“Forms of encryption can be traced as far back as ancient Egypt, using non-standard hieroglyphs.”

“Making data impossible to read is just one step, you also need the key to decrypt that data.”

“The universe is 14 billion years old, but it would take seven times that time to crack 256-bit encryption.”

ENCRYPTION

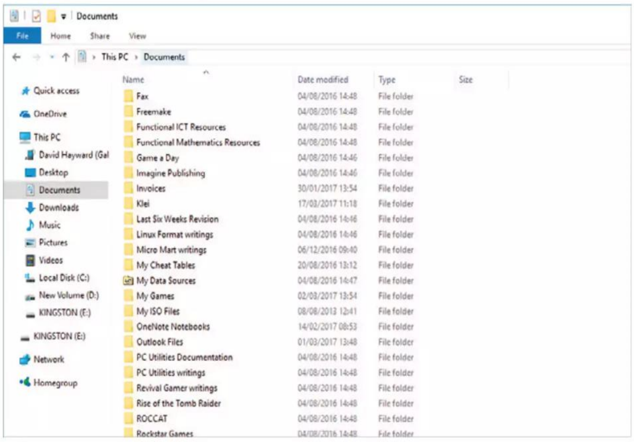
Encrypting Your Windows 10 Laptop

Windows 10 Pro comes with Microsoft's BitLocker program to encrypt the file system; however, Windows 10 Home versions do not have this feature. Thankfully there are many encryption programs available for download, we're using DiskCryptor in this tutorial.

Windows 10, Under Lock and Key

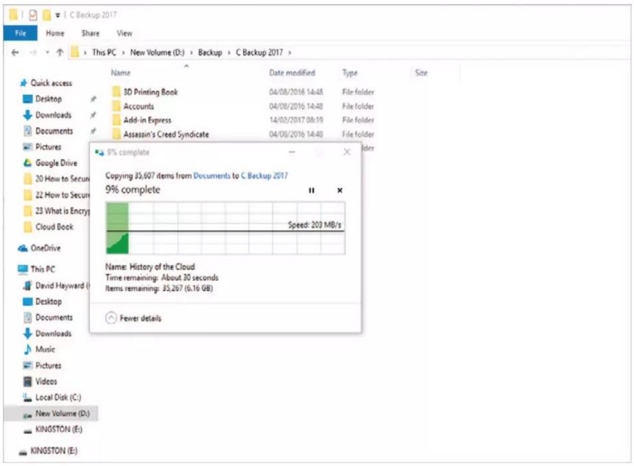
We're going to encrypt a 2GB USB flash in this example, purely for ease of use and to demonstrate how you can encrypt your entire laptop hard drive(s).

STEP 1 Encryption doesn't affect the core data, other than making it impossible to read without the decryption key but it's always worth making sure you have a backup of all your data prior to any system related changes. If you store your work or data in the Documents folder, then start by opening it in Windows Explorer.


Documents
File
Home
Share
View
This PC › Documents
Quick access
OneDrive
This PC
David Hayward (Gal
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
New Volume (D:)
KINGSTON (E:)
KINGSTON (E:)
Network
Homegroup

Name	Date modified	Type	Size
Fax	04/08/2016 14:48	File folder	
Freemake	04/08/2016 14:48	File folder	
Functional ICT Resources	04/08/2016 14:48	File folder	
Functional Mathematics Resources	04/08/2016 14:48	File folder	
Game a Day	04/08/2016 14:46	File folder	
Imagine Publishing	04/08/2016 14:46	File folder	
Invoices	30/01/2017 13:54	File folder	
Klei	17/03/2017 11:18	File folder	
Last Six Weeks Revision	04/08/2016 14:46	File folder	
Linux Format writings	04/08/2016 14:46	File folder	
Micro Mart writings	06/12/2016 09:40	File folder	
My Cheat Tables	20/08/2016 13:12	File folder	
My Data Sources	04/08/2016 14:47	File folder	
My Games	02/03/2017 13:54	File folder	
My ISO Files	08/08/2013 12:41	File folder	
OneNote Notebooks	14/02/2017 08:53	File folder	
Outlook Files	01/03/2017 13:48	File folder	
PC Utilities Documentation	04/08/2016 14:48	File folder	
PC Utilities writings	04/08/2016 14:48	File folder	
Revival Gamer writings	04/08/2016 14:48	File folder	
Rise of the Tomb Raider	04/08/2016 14:48	File folder	
ROCCAT	04/08/2016 14:48	File folder	
Rockstar Games	04/08/2016 14:48	File folder	

STEP 2 Press Ctrl+A to highlight all the files, then press Ctrl+C to copy them to the clipboard. Next, choose a suitable backup location such as an external or network drive and when ready, press Ctrl+V to paste the copied data into the new location. Then, should something go wrong, you have a recent backup of your most used data.


C Backup 2017
File
Home
Share
View
This PC › New Volume (D:) › Backup › C Backup 2017 ›
Quick access
Desktop
Downloads
Documents
Pictures
Google Drive
20 How to Secur
22 How to Secur
23 What is Encry
Cloud Book
OneDrive
This PC
David Hayward (
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
New Volume (D:)
KINGSTON (E:)
KINGSTON (E:)
9% complete
Fewer details

Name	Date modified	Type	Size
3D Printing Book	04/08/2016 14:48	File folder	
Accounts	04/08/2016 14:48	File folder	
Add-in Express	14/02/2017 08:19	File folder	
Assassin's Creed Syndicate	04/08/2016 14:48	File folder	

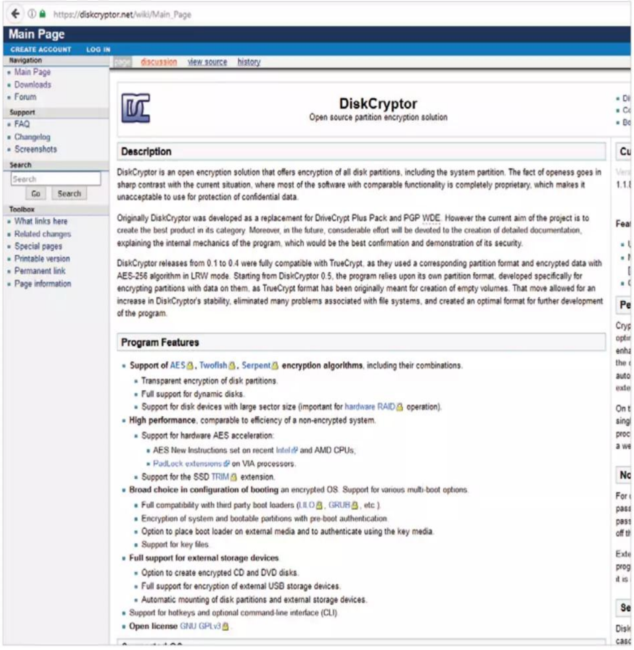
Copying 35,607 items from Documents to C Backup 2017

9% complete

Speed: 203 MB/s

Name: History of the Cloud
Time remaining: About 30 seconds
Items remaining: 35,267 (6.16 GB)

STEP 3 It's always best to ensure safe data before commencing with anything like this. It's also always worth doing (as we are) a test of the software first, on a disk that you don't mind messing up should you get the process wrong. Let's start by navigating to the DiskCryptor homepage, at www.diskcryptor.net/wiki/Main_Page.


https://diskcryptor.net/wiki/Main_Page
Main Page
CREATE ACCOUNT
LOG IN
Navigation
Main Page
Downloads
Forum
Support
FAQ
Changelog
Screenshots
Search
Go
Search
Toolbox
What links here
Related changes
Special pages
Printable version
Permanent link
Page information
discussion
view source
history

DiskCryptor
Open source partition encryption solution

Description

DiskCryptor is an open encryption solution that offers encryption of all disk partitions, including the system partition. The fact of openess goes in sharp contrast with the current situation, where most of the software with comparable functionality is completely proprietary, which makes it unacceptable to use for protection of confidential data.

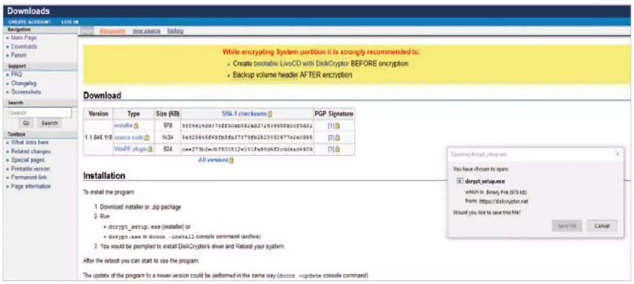
Originally DiskCryptor was developed as a replacement for DriveCrypt Plus Pack and PGP WDE. However the current aim of the project is to create the best product in its category. Moreover, in the future, considerable effort will be devoted to the creation of detailed documentation, explaining the internal mechanics of the program, which would be the best confirmation and demonstration of its security.

DiskCryptor releases from 0.1 to 0.4 were fully compatible with TrueCrypt, as they used a corresponding partition format and encrypted data with AES-256 algorithm in LRW mode. Starting from DiskCryptor 0.5, the program relies upon its own partition format, developed specifically for encrypting partitions with data on them, as TrueCrypt format has been originally meant for creation of empty volumes. That move allowed for an increase in DiskCryptor's stability, eliminated many problems associated with file systems, and created an optimal format for further development of the program.

Program Features

- **Support of AES, Twofish, Serpent encryption algorithms**, including their combinations.
  - Transparent encryption of disk partitions.
  - Full support for dynamic disks.
  - Support for disk devices with large sector size (important for hardware RAID operation).
- **High performance**, comparable to efficiency of a non-encrypted system.
  - Support for hardware AES acceleration:
    - AES New Instructions set on recent Intel and AMD CPUs;
    - PadLock extensions on VIA processors.
  - Support for the SSD TRIM extension.
- **Broad choice in configuration of booting** an encrypted OS. Support for various multi-boot options.
  - Full compatibility with third party boot loaders (LILO, GRUB, etc.)
  - Encryption of system and bootable partitions with pre-boot authentication.
  - Option to place boot loader on external media and to authenticate using the key media.
  - Support for key files.
- **Full support for external storage devices**
  - Option to create encrypted CD and DVD disks.
  - Full support for encryption of external USB storage devices.
  - Automatic mounting of disk partitions and external storage devices.
- Support for hotkeys and optional command-line interface (CLI).
- **Open license** GNU GPLv3.

STEP 4 Using the menu to the top left, click on the Downloads link. Look for the latest version in the Download section and click the link for the Installer. This will open a confirmation box, click the Save File button to download the DiskCryptor executable file.


Downloads
CREATE ACCOUNT
LOG IN
Navigation
Main Page
Downloads
Forum
Support
FAQ
Changelog
Screenshots
Search
Go
Search
Toolbox
What links here
Related changes
Special pages
Printable version
Permanent link
Page information
discussion
view source
history
Cancel

While encrypting System partition it is strongly recommended to:
- Create bootable LiveCD with DiskCryptor BEFORE encryption
- Backup volume header AFTER encryption

Download

Version	Type	Size (KB)	SHA-1 checksums	PGP Signature
1.1.846.118	installer	978	[illegible]	[1]
	source code	1434	[illegible]	[2]
	WinPE plugin	824	[illegible]	[1]

All versions

Installation

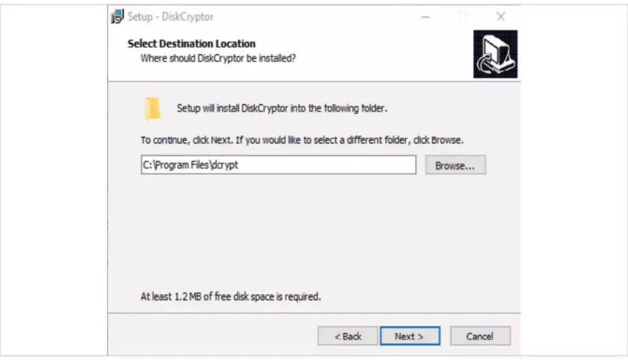
To install the program:

1. Download installer or zip package
2. Run
   - dcrypt_setup.exe (installer) or
   - dcrypt.exe or dccon -install console command (archive)
3. You would be prompted to install DiskCryptor's driver and Reboot your system.

After the reboot you can start to use the program.

The update of the program to a newer version could be performed in the same way (dccon -update console command)

STEP 5 The dcrypt_setup.exe file should now be in your Downloads folder. Double-click it and select Yes to accept the Windows confirmation. With the DiskCryptor setup window open, click the Next button and accept the license agreement on the following page. For the remainder of the options choose the defaults, clicking Next. When done, click the Install button and reboot the computer.


Setup - DiskCryptor
Select Destination Location
Where should DiskCryptor be installed?
Browse...
< Back
Next >
Cancel

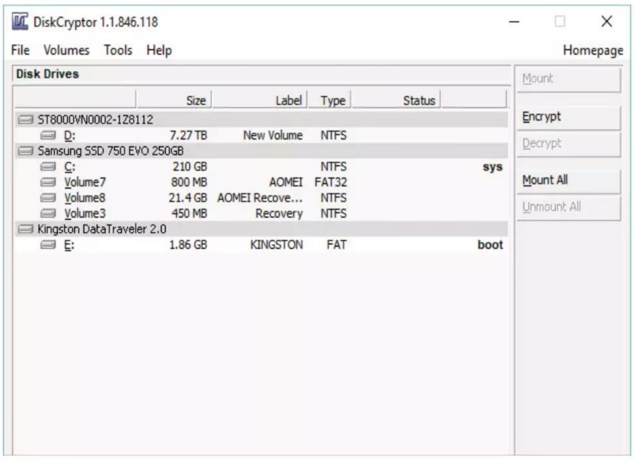
Setup will install DiskCryptor into the following folder.

To continue, click Next. If you would like to select a different folder, click Browse.

C:\Program Files\dcrypt

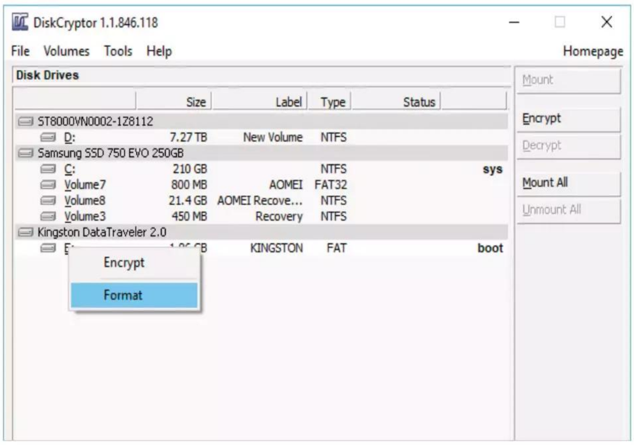
At least 1.2 MB of free disk space is required.

STEP 6 After a reboot, click the Windows Start button and locate the newly installed DiskCryptor program. You will need to click Yes to authorise its administrative access. With DiskCryptor open you can see the list of currently installed hard drives in your system. You can click each in turn and view its information at the bottom of the DiskCryptor window.


DiskCryptor 1.1.846.118
File
Volumes
Tools
Help
Homepage
Disk Drives
Mount
Encrypt
Decrypt
Mount All
Unmount All

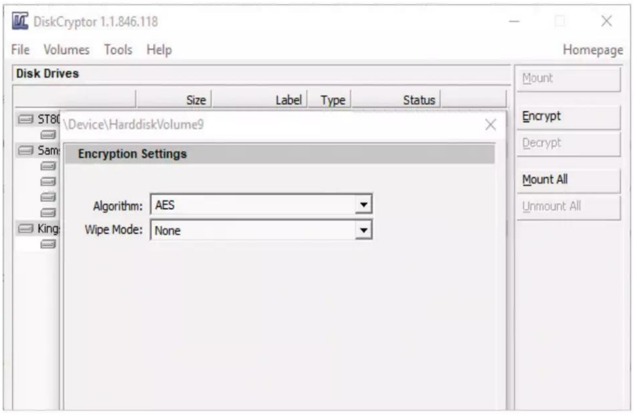
	Size	Label	Type	Status	
ST8000VN0002-1Z8112					
D:	7.27 TB	New Volume	NTFS		
Samsung SSD 750 EVO 250GB					
C:	210 GB		NTFS		sys
Volume7	800 MB	AOMEI	FAT32		
Volume8	21.4 GB	AOMEI Recove...	NTFS		
Volume3	450 MB	Recovery	NTFS		
Kingston DataTraveler 2.0					
E:	1.86 GB	KINGSTON	FAT		boot

STEP 7 Start by selecting the disk you want to encrypt. In our example, as mentioned before, we're going to test this out on a USB stick. We recommend you do too, until you're comfortable with the process. With the correct drive selected, either click the Encrypt button to the right or right-click and choose Encrypt from the menu.


DiskCryptor 1.1.846.118
File
Volumes
Tools
Help
Homepage
Disk Drives
Mount
Encrypt
Decrypt
Mount All
Unmount All
Encrypt
Format

	Size	Label	Type	Status	
ST8000VN0002-1Z8112					
D:	7.27 TB	New Volume	NTFS		
Samsung SSD 750 EVO 250GB					
C:	210 GB		NTFS		sys
Volume7	800 MB	AOMEI	FAT32		
Volume8	21.4 GB	AOMEI Recove...	NTFS		
Volume3	450 MB	Recovery	NTFS		
Kingston DataTraveler 2.0					
E:	1.86 GB	KINGSTON	FAT		boot

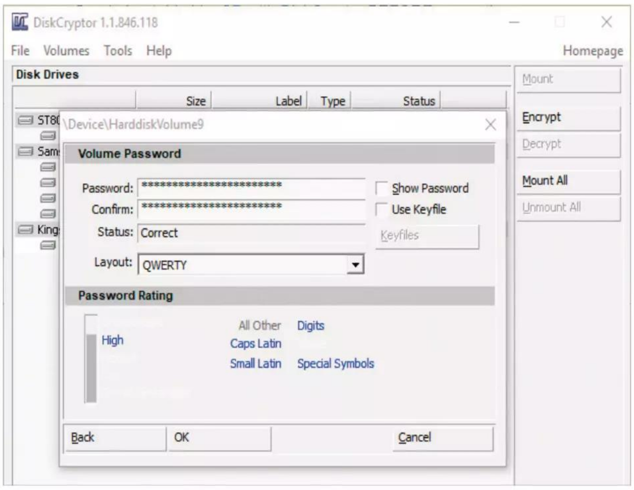
STEP 8 You're now offered a selection of available algorithms to choose from. Click the drop-down box to view them all but we recommend staying with the default AES algorithm for the time being. Leave the Wipe Mode box as None and when you're ready, click the Next button.


DiskCryptor 1.1.846.118
File
Volumes
Tools
Help
Homepage
Disk Drives
Size
Label
Type
Status
Mount
Encrypt
Decrypt
Mount All
Unmount All
\Device\HarddiskVolume9
Encryption Settings

Algorithm: AES

Wipe Mode: None

STEP 9 In the next section, choose a unique password for accessing the encrypted disk; you're notified how strong the password is. When you're ready, enter it again in the Confirm box. Click the OK box to start the encryption process.


DiskCryptor 1.1.846.118
File
Volumes
Tools
Help
Homepage
Disk Drives
Mount
Encrypt
Decrypt
Mount All
Unmount All
\Device\HarddiskVolume9
Volume Password
Show Password
Use Keyfile
Keyfiles
Password Rating
High
All Other
Digits
Caps Latin
Small Latin
Special Symbols
Back
OK
Cancel

Password: ************************

Confirm: ************************

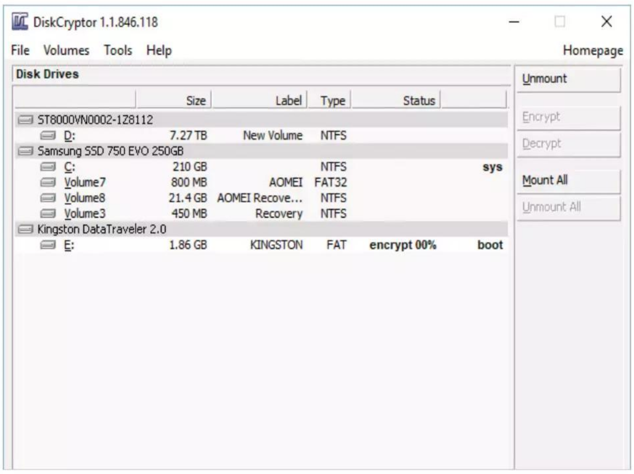
☐ Show Password

☐ Use Keyfile

Status: Correct

Layout: QWERTY

STEP 10 Depending on the size of the drive, and how much data there is on it, the encryption process could take some time. When it's complete you're notified and the selected drive will the fully encrypted, with you being to access and decrypt it using the password you set up in the previous step.


DiskCryptor 1.1.846.118
File
Volumes
Tools
Help
Homepage
Disk Drives
Unmount
Encrypt
Decrypt
Mount All
Unmount All

	Size	Label	Type	Status	
ST8000VN0002-1Z8112					
D:	7.27 TB	New Volume	NTFS		
Samsung SSD 750 EVO 250GB					
C:	210 GB		NTFS		sys
Volume7	800 MB	AOMEI	FAT32		
Volume8	21.4 GB	AOMEI Recove...	NTFS		
Volume3	450 MB	Recovery	NTFS		
Kingston DataTraveler 2.0					
E:	1.86 GB	KINGSTON	FAT	encrypt 00%	boot

Top Ten Encryption Tools for Windows 10

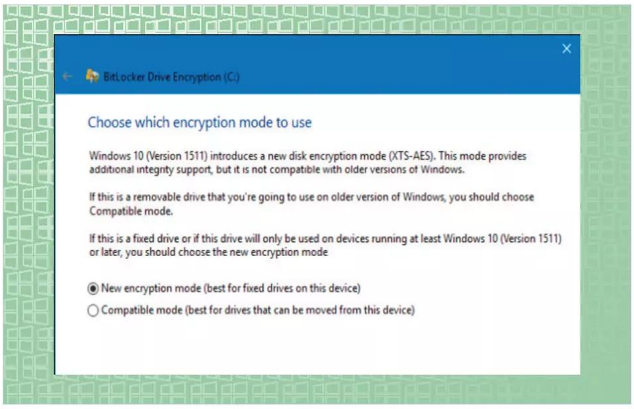
There's no shortage of programs that can encrypt files, folders and entire drives for Windows 10. Whilst some are very good indeed, others tend to fall by the wayside by not offering as good a solution.

Encryption Galore

Here are ten different encryption tools for you to consider that work well with Windows 10, and some previous versions too. Some are free, others cost but they're all good in their own right.

BITLOCKER

Available only for users of Windows 10 Pro, Windows 8.1 Pro and Enterprise and Windows 7 Enterprise and Ultimate versions. If you're running the Home versions, you'll need to upgrade via the Microsoft site, or from the Windows Store. In short, BitLocker offers full disk encryption with 128-bit or 256-bit AES standards.



Choose which encryption mode to use

Windows 10 (Version 1511) introduces a new disk encryption mode (XTS-AES). This mode provides additional integrity support, but it is not compatible with older versions of Windows.

If this is a removable drive that you're going to use on older version of Windows, you should choose Compatible mode.

If this is a fixed drive or if this drive will only be used on devices running at least Windows 10 (Version 1511) or later, you should choose the new encryption mode

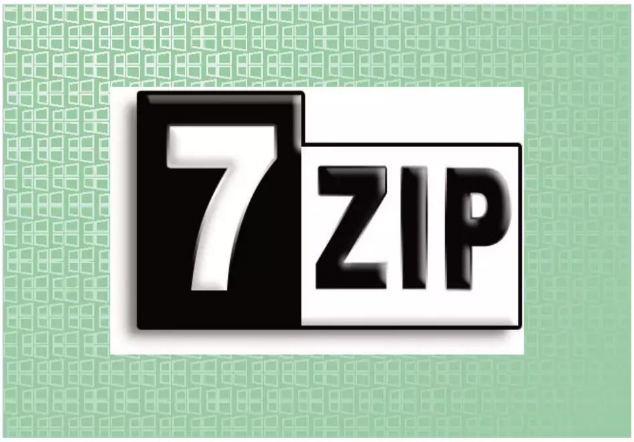
● New encryption mode (best for fixed drives on this device)
○ Compatible mode (best for drives that can be moved from this device)

VERACRYPT

This is a free disk encryption program that's based on the popular TrueCrypt. It offers enhanced security, lots of levels of encryption and support for UEFI drives. It's available for Windows version 7 onwards as well as Mac OS X, Linux and even the Raspberry Pi.

7-ZIP

Primarily a compression program, 7-Zip can also encrypt your data with the AES 256-bit standard. It's simple to use, completely free and comes in either 32-bit or 64-bit versions depending on which type your core Windows system is.



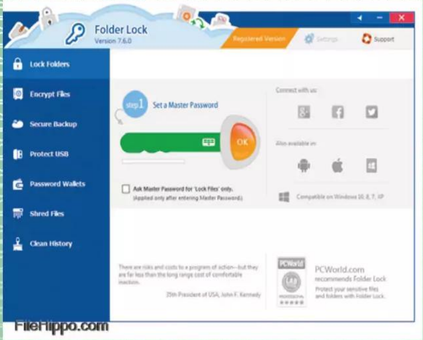
AXCRYPT

Another excellent free program, AxCrypt offers 256-bit encryption, easy to use interface, cloud storage integration, password management, secured folders and is available in a multitude of different languages. There's support for Windows Vista onward as well as support for files sizes over 4GB.

AxCrypt
www.axcrypt.net

FOLDER LOCK

An excellent and comprehensive folder locking program, with support for 256-bit encryption and Windows versions from Vista onward. It costs in the region of £40 but you'll need to check for the most recent pricing. For your money, you get secure backups, USB protection, password wallets, a secure file shredder and much more.


Folder Lock
Version 7.6.0
Registered Version
Settings
Support
Lock Folders
Encrypt Files
Secure Backup
Protect USB
Password Wallets
Shred Files
Clean History
step 1
Set a Master Password
OK
Ask Master Password for 'Lock Files' only.
(Applied only after entering Master Password)
Connect with us:
Also available in:
Compatible on Windows 10, 8, 7, XP
PCWorld
PCWorld.com
recommends Folder Lock
FileHippo.com

CRYPTOEXPERT 8

Costing around £60, CryptoExpert 8 offer support for Windows versions from 7 onward, unlimited file size encryption, 256-bit AES encryption, unlimited secure file vaults and on the fly encryption as you move and copy files around your system.

CryptoExpert 8
Secure data vaults for Windows

CERTAINSAFE

This is an interesting product, as it provides cloud-based encryption for any files or folders you upload into your online storage. It offers AES 256-bit encryption and an easy to use setup and integration into your cloud provider. It's Pay as you Go, so you only pay for what you use.

CertainSafe

GPG4WIN

This entry is a little more advanced but once you master its intricacies it's an extraordinarily powerful program, and free. It's designed for file and email encryption, offering incredible levels of security for Windows 7 upwards and Microsoft Outlook 2003 and newer.

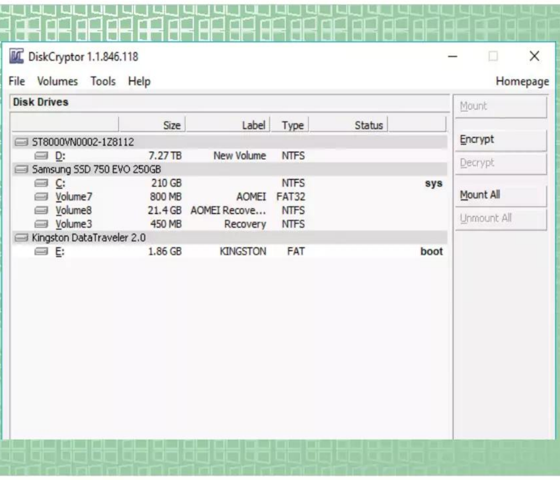
DEKART PRIVATE DISK

This is a simple and easy to use program that supports AES 256-bit encryption, compatibility with Windows Mobile, free unlimited support and updates; and it also includes its own firewall to help prevent hackers from gaining access to your system.

dekart
MAKE IT SECURE

DISKCRYPTOR

We used DiskCryptor in the previous tutorial as it's a fairly straightforward program that can achieve high levels of encryption with ease. There's a lot more you can do with it and you can get further support from within the product's homepage.


DiskCryptor 1.1.846.118
File
Volumes
Tools
Help
Homepage
Disk Drives
Mount
Encrypt
Decrypt
Mount All
Unmount All

	Size	Label	Type	Status	
ST8000VN0002-1Z8112					
D:	7.27 TB	New Volume	NTFS		
Samsung SSD 750 EVO 250GB					
C:	210 GB		NTFS		sys
Volume7	800 MB	AOMEI	FAT32		
Volume8	21.4 GB	AOMEI Recove...	NTFS		
Volume3	450 MB	Recovery	NTFS		
Kingston DataTraveler 2.0					
E:	1.86 GB	KINGSTON	FAT		boot

What is a VPN?

Your system may be secure to any online threats but it doesn't always mean your privacy is assured. This is where a VPN comes in, as it offers the user a heightened level of anonymity when online and even another level of security and protection.

Virtual Private Network

Using a VPN can help hide your online presence. Whilst this may seem like an ideal way to get to illegal content, it's actually designed to help fight for your basic right to Internet and digital privacy.

Essentially, a VPN (Virtual Private Network) is a server or group of servers in a remote location that you can connect to through a client. The VPN servers then hide your Internet-bound IP address with their own, so if you connected to a VPN that's located in Australia then your IP address would be as if you were actually sat at a desktop down under.

The benefits of this are many but mainly a VPN will allow you to access region restricted websites, protect you from tracking and shield your browsing activities from those who want to find out where you are personally based. Obviously there comes a negative side, in the form of being able to access content that your country has deemed illegal for some reason but on the positive, VPNs have allowed people in countries with extraordinarily tight restrictions to get access to the outside world; often enabling them to report on what's going on in their own country to the world.

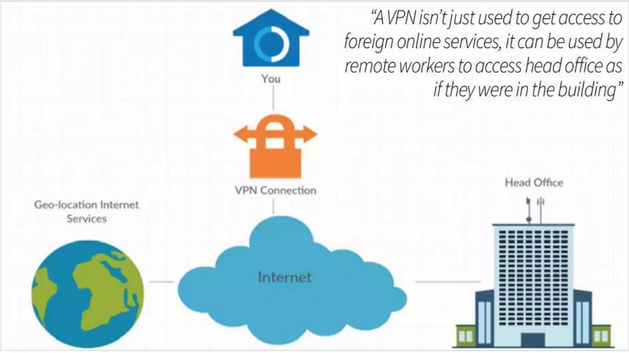
However, for most users having a VPN means they're able to gain access to TV channels in the U.S., Canada, Europe and other parts of the world. It's not always about being able to moderately 'cheat the system' by forcing the Internet to think you're somewhere else other than where you actually are though. Remote workers and employees who live in other countries can connect to company VPNs and be able to use the company's network resources as if they were physically sat in the building.

The connection from your computer to the VPN server, via the client, is usually secure to the tune of 256-bit encryption levels, depending on the VPN company who is hosting the service. All your Internet traffic will filter through the VPN server's systems, offering multiple layers of protection from viruses, malware and privacy. Beyond the other possible scenarios, using a VPN whilst you're abroad, working in a hotel for example, will enable you to access your home country's services and work resources. One more element that's worth mentioning is that using Wi-Fi hotspots is one of the biggest security risk for travellers; using a VPN can effectively improve your security whilst using a café's free Wi-Fi.

Most operating systems come with the ability to connect to a VPN through their network settings. If you have the network and connection details of the VPN in question, then you're able to connect to it using the built-in Windows 10, Linux or macOS options. However, the more common, and in some respects, easier method, is to use the client which most VPNs now offer as standard. The client is often simply a connection window that will ask you your login details, then provide a method of allowing you to connect to any of provider's geo-location servers, listed by country. Once the choice is made, you simply click the connect box and within a few seconds your IP address will be located within the chosen country.

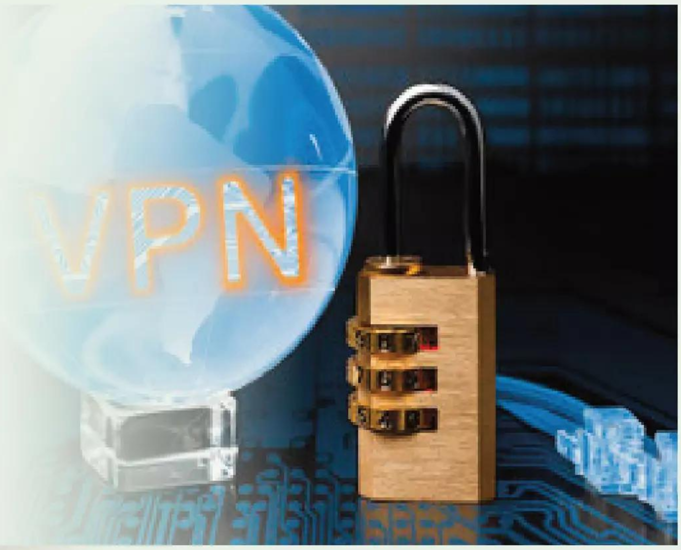
There are plenty of VPN providers to choose from and we'll look at ten of the most popular in a while. Some offer a free connection service that's handy for quick browsing but isn't very fast. To gain access to faster servers, with better security and protection features you need to pay a monthly or annual subscription fee. Thankfully it's not a lot, for the most part: you'll be expected to pay in the region of £5 to £15 per month. This grants you better coverage and the ability to use up to five or more different devices, including tablets and phones.

Over the coming pages we dig a little deeper into VPNs, as you can imagine, using one will significantly improve your protection when online. In terms of Windows 10 security, the use of a VPN is quickly becoming vital, so by the end of this chapter you'll be knowledgeable and helpfully utilising one to your own advantage.

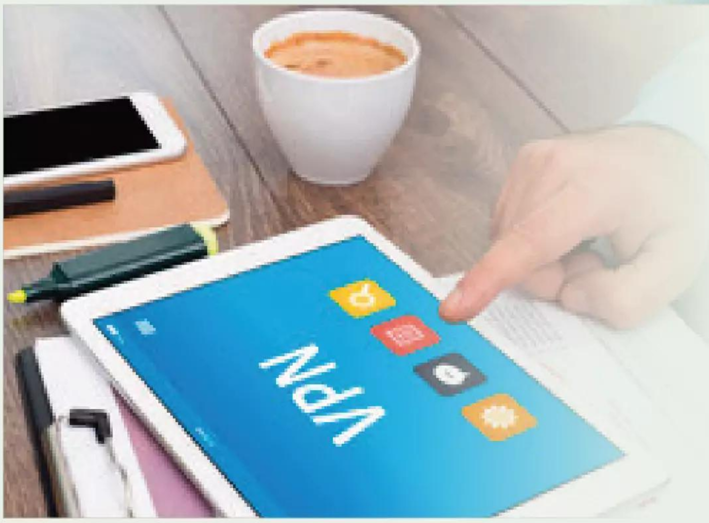


"A VPN isn't just used to get access to foreign online services, it can be used by remote workers to access head office as if they were in the building"

> *Using a VPN will protect your access online and filter all your Internet traffic through its secure service.*



"You're able to access web pages and Internet services from all over the world, even if you can't from your own country."



"A VPN greatly improves security for devices and when you're using free Wi-Fi at cafés and other such locations."

How Can a VPN Improve Windows Security?

We've emphasised the enhanced privacy that a VPN offers when you're connected to its services, and the heightened levels of anonymity, but what security benefits does a VPN bring to a Windows 10 computer with an antivirus program already installed?

Security Beyond Anonymity

It's a good question: how can a VPN improve Windows security? Whilst the privacy side is well catered for, there are some good security enhancements and features a VPN brings to the table.

BROWSING ACTIVITY

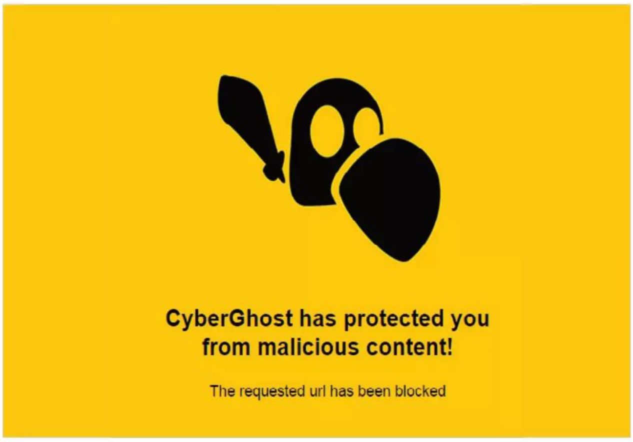
This doesn't happen often but an ISP can become compromised and details of user activities leaked or stolen. Using a VPN can hide your browsing activity from trackers and even your ISP, enabling you to browse with freedom of fear of having your details leaked or accessed by others.

ANTIMALWARE

Many VPN providers utilise a level of antimalware into their security layers. This enhances your security by filtering any downloads through the VPN first. Should there be a virus present, then it can be removed or stopped at the VPN before it even reaches you.

THREAT PROTECTION

To expand the previous feature, VPNs will filter web pages that are dangerous or contain threats. Even with a good antivirus client installed, you can still access a dangerous site. Using a VPN will stop the site from even being loaded.



CyberGhost has protected you from malicious content!

The requested url has been blocked

HIGHEST ENCRYPTION

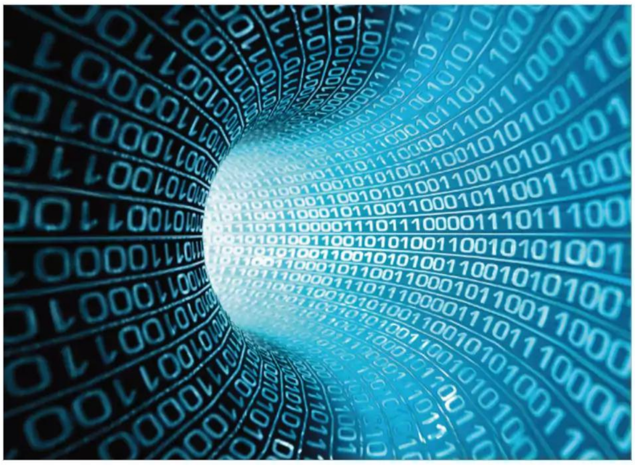
The connection between you and the VPN server is encrypted to the highest possible standards. This makes it near impossible for some external element to gain access to the data you're transmitting. Online banking and shopping are extremely secure with a VPN.

WI-FI PROTECTION

Public and free Wi-Fi hotspots are notorious when it comes to mobile security. Anyone with a little knowledge and some free tools via the Internet can intercept public Wi-Fi network and hijack your connection, revealing all your data. A VPN will encrypt the data and protect you.

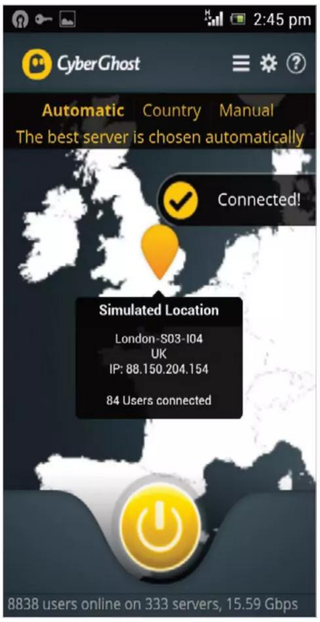
SECURE TUNNEL

If you're working abroad, or you're a remote worker, then a VPN connection to the company's servers will ensure that all the sensitive business data will remain secure. It's difficult for a company to ensure 100 per cent security with mobile and off-site workers but a VPN will provide a secure tunnel straight to the company itself.



MULTI-PLATFORM

The availability of iOS and Android VPN clients means that your call data and data stored on your device is also secure. Mobile VPN apps will use the same levels of protection and security, so your data can't be stolen when you're not even aware of it.

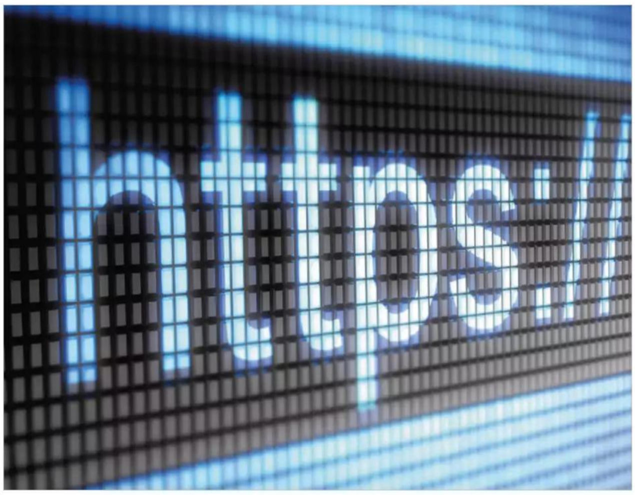

2:45 pm
CyberGhost
Automatic
Country
Manual
The best server is chosen automatically
Connected!
Simulated Location
London-S03-I04
UK
IP: 88.150.204.154
84 Users connected
8838 users online on 333 servers, 15.59 Gbps

AD BLOCKING

Most VPNs will also add an extra layer of security whereby they actively block any advertising from websites. Internet ads are a necessary evil in some ways, as they provide much needed funds for your favourite freely available websites. However, some contain malicious content and need to be blocked.

USE HTTPS

Using HTTPS instead of HTTP uses the secure side of the Internet protocol. Sadly, it's not always implemented in browsers or by users. Many VPNs will force all websites to use the secure connection that a HTTPS site offers, enhancing your browsing security.



ZERO LOGS

In some countries data retention laws are quite archaic, with governments and other bodies being able to access your data log for as long as you've been able to access the Internet. A good VPN won't detail any logs of your browsing and in most cases won't even hand over any personal information relating to you to other agencies.

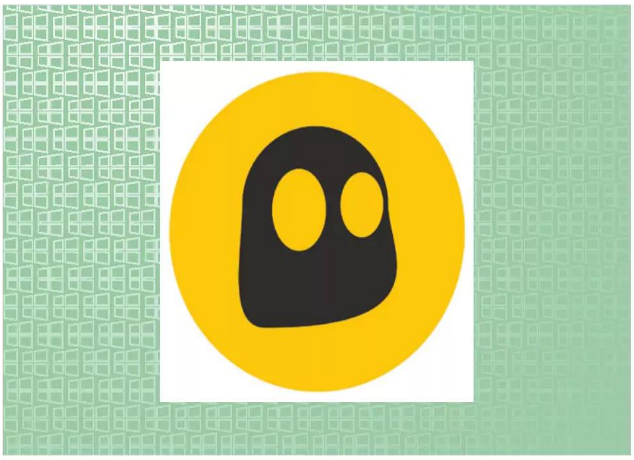
Top Ten VPNs

There's no shortage of programs that can encrypt files, folders and entire drives for Windows 10. Whilst some are very good indeed, others tend to fall by the wayside by not offering as good a solution.

Encryption Galore

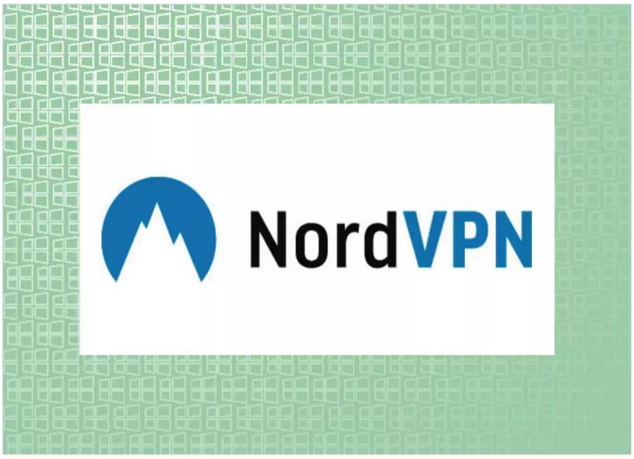
Here are ten different encryption tools for you to consider that work well with Windows 10, and some previous versions too. Some are free, others cost but they're all good in their own right.

CYBERGHOST CyberGhost is our favourite VPN. It offers 256-bit AES military grade encryption, no logging, access to 27 countries and hundreds of servers, protected browsing, ad blocking, access to fast servers, unlimited traffic and bandwidth and an anti-fingerprint system. All for around £5.83 per month for up to five devices.



HMA Despite its colourful name, Hide My Ass VPN is considered to be one of the best services available. Along with the usual secure 256-bit encryption connection you get blistering speeds, access to over 300 locations, anonymous email use, a free web proxy access and free extensions for your browser. Expect to pay around £5 per month.

NORDVPN NordVPN offers two levels of encryption, access to fast servers, no logging, a kill switch in case the VPN connection drops and you're still surfing and support for multiple devices and operating systems. It's well priced and is highly regarded among the press and media. Not bad for a mere $5.75 per month (around £4.50).



PUREVPN With support for multiple devices, 256-bit AES encryption and access to 180 locations worldwide with 750 plus servers, PureVPN is a great choice for the home user. The cost varies depending on the package but expect to pay in the region of $5.90 (around £4.58). Just as with all these VPNs, it's worth checking for the latest pricing.

VPN UNLIMITED

VPN Unlimited offers a full firewall service with anti-malware, ad blocking and anti-tracking. There's 256-bit AES encryption, over a thousand servers in 70-plus locations, support for up to five devices, fast servers and app support for iOS, Android and Widows Phone. Pricing varies but expect to pay around $8.99 (approx. £6.97) per month.

IPVANISH

IPVanish is another highly regarded and awarded VPN service. For $6.49 (around £5) per month depending on the package, you get access to fast servers, unlimited bandwidth, no logging, 256-bit AES encryption and support for up to five different devices.

TUNNELBEAR VPN

TunnelBear VPN offers an initial 500MB per month free service, moving up to $9.99 (around £7.75) per month for unlimited bandwidth. For this you get access to fast servers across twenty plus countries, 256-bit AES encryption and support for Windows, iOS, Android, macOS and browser add-ons.

TunnelBear

PRIVATE INTERNET ACCESS

Private Internet Access VPN offers a wealth of features with its impressive service. 256-bit levels of encryption, no traffic logging, ad blocking, support for five devices and access to over three thousand servers across twenty five countries. It's surprisingly cheap too, at just $6.95 (about £5.40) per month depending on the package you opt for.

VYPRVPN

VyprVPN is an exceptionally good service that offer access to fast servers, multiple device support, unlimited bandwidth and connection, 256-bit AES encryption and access to over seventy global locations and hundreds of servers. The Premium package costs just £5.83 per month for a one year subscription, but check regularly for any changes.

FACELESS.ME

Faceless Me is an interestingly named VPN service. Amongst its features expect to see elevated levels of encryption, unrestricted access, an easy to use interface and unlimited traffic. You get 2GB per month for free but for $6.65 (around £5.16) you can have unlimited access and traffic.

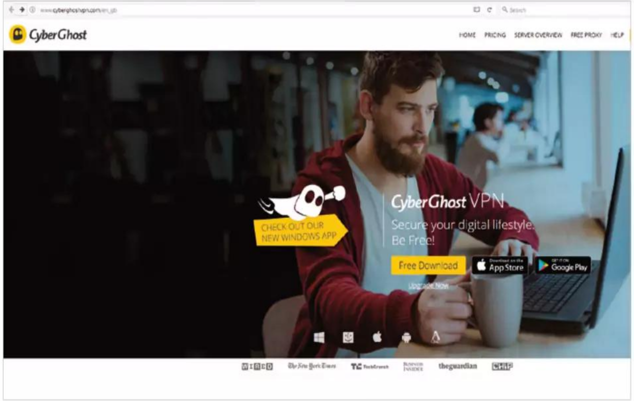
Using a VPN for Added Security and Privacy

We've covered how a VPN works, how it can improve your security and given you a top ten chart of recommended providers but we've not looked at how you would set one up and what it's like when up and running.

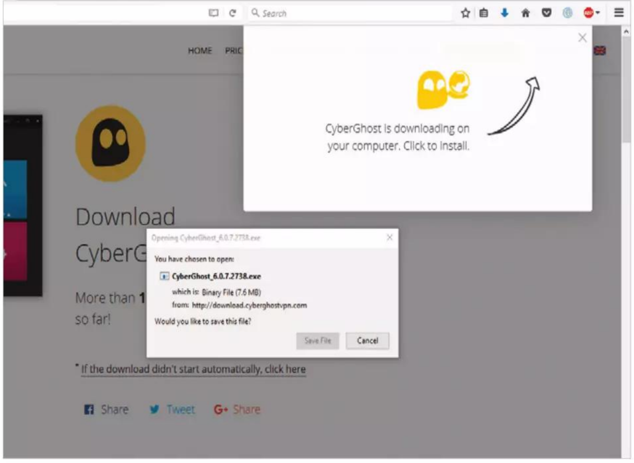
CyberGhost

We're going to use CyberGhost as the example VPN for this tutorial. You'll need to purchase one of the available packages to begin with, Premium is £3.74 per month, while Premium Plus is £5.83.

STEP 1 We won't use the free option in this instance, as the paid for services offer a better set of features with which to display the VPN in action. Start by navigating to www.cyberghostvpn.com and clicking on the Pricing link in the upper portion of the main CyberGhost site for your regional and latest pricing.


CyberGhost
HOME
PRICING
SERVER OVERVIEW
FREE PROXY
HELP
CHECK OUT OUR NEW WINDOWS APP
CyberGhost VPN
Secure your digital lifestyle.
Be Free!
Free Download
App Store
Google Play
Upgrade Now
WIRED
The New York Times
TC TechCrunch
Business Insider
theguardian
CHIP

STEP 2 Assuming you've purchased one of the options, click the yellow Free Download button located in the top right of the main page. This will, after a few seconds, automatically initialise the download of the latest CyberGhost client software. Click Save File to download it to your Downloads folder.


Search
HOME
PRIC
Download
CyberG
More than 1
so far!
Save File
Cancel
Share
Tweet
G+ Share

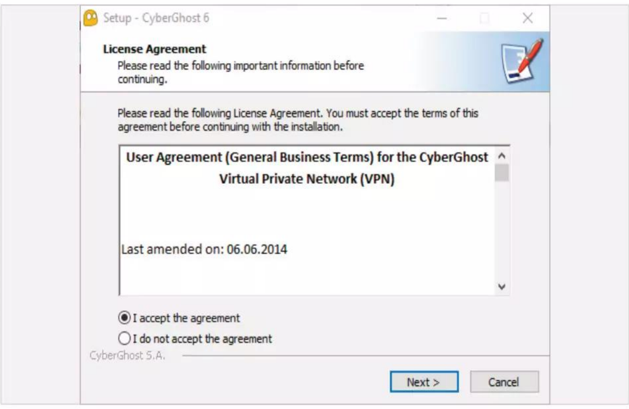
CyberGhost is downloading on your computer. Click to install.

Opening CyberGhost_6.0.7.2738.exe

You have chosen to open:
CyberGhost_6.0.7.2738.exe
which is: Binary File (7.6 MB)
from: http://download.cyberghostvpn.com
Would you like to save this file?

* If the download didn't start automatically, click here

STEP 3 Go to the Downloads folder and double click the CyberGhost executable followed by a click on Yes for the Windows authentication process. Accept the agreement and follow the on-screen instructions to set up CyberGhost on your PC; the default options are fine to use, unless you specifically require a different location for installation.


Setup - CyberGhost 6
Next >
Cancel

License Agreement
Please read the following important information before continuing.

Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.

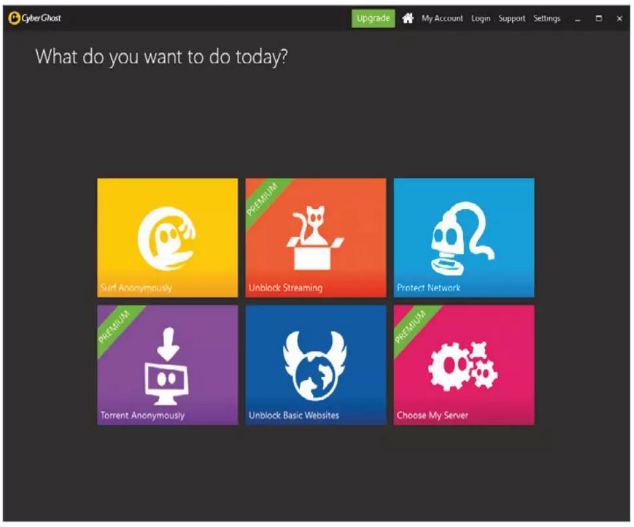
User Agreement (General Business Terms) for the CyberGhost Virtual Private Network (VPN)

Last amended on: 06.06.2014

● I accept the agreement
○ I do not accept the agreement

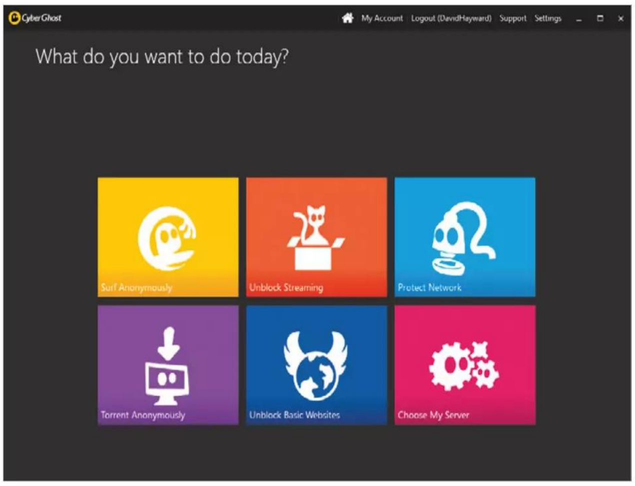
CyberGhost S.A.

STEP 4 Once the installation is complete you're presented with the main CyberGhost client window. However, before you make a connection, click on the Login link located at the top of the client window.

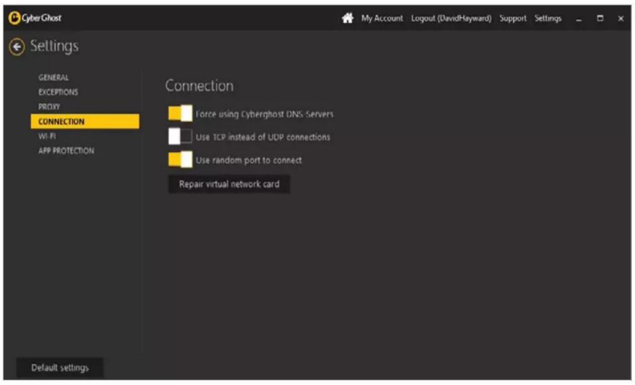

CyberGhost
Upgrade
My Account
Login
Support
Settings
Surf Anonymously
PREMIUM
Unblock Streaming
Protect Network
PREMIUM
Torrent Anonymously
Unblock Basic Websites
PREMIUM
Choose My Server

What do you want to do today?

STEP 5 Enter your CyberGhost login and password that you set up when you purchased the package and click the OK button. Once the login is confirmed you're taken back to the main client window where the available options for the account package you purchased will be displayed.


CyberGhost
My Account
Logout (DavidHayward)
Support
Settings
What do you want to do today?
Surf Anonymously
Unblock Streaming
Protect Network
Torrent Anonymously
Unblock Basic Websites
Choose My Server

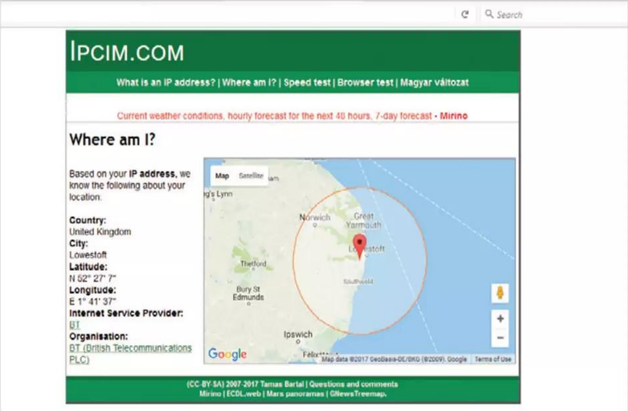
STEP 6 Before you use the service, it's best to check a couple of things. First click on the Settings link along the top of the client window. In here you can see multiple options for the control, connection and how CyberGhost will work with your PC. Generally speaking, the defaults are fine unless you have a specific reason to change them.


CyberGhost
My Account
Logout (DavidHayward)
Support
Settings
Settings
GENERAL
EXCEPTIONS
PROXY
CONNECTION
WI-FI
APP PROTECTION
Repair virtual network card
Default settings

Connection

- ☑ Force using Cyberghost DNS-Servers
- ☐ Use TCP instead of UDP connections
- ☑ Use random port to connect

STEP 7 One more thing before connecting to the CyberGhost VPN: open a browser and enter www.ipcim.com/en/?p=where. This will display detailed information based on your IP address, such as the ISP you're using, the country, city, even latitude and longitude, complete with a map and possible radius you fall into. This is the kind of information we want to secure from prying eyes.

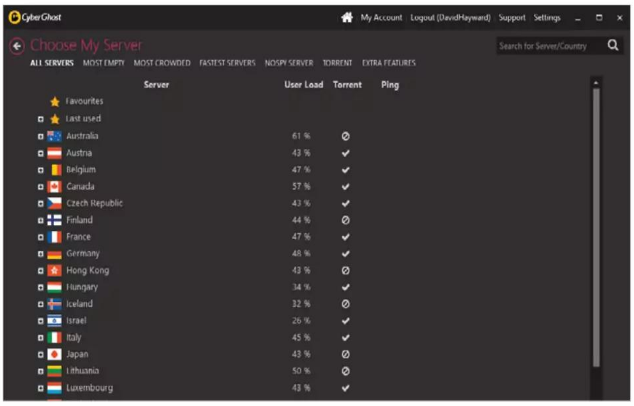

Search
IPCIM.COM
What is an IP address? | Where am I? | Speed test | Browser test | Magyar változat
Current weather conditions, hourly forecast for the next 48 hours, 7-day forecast - Mirino
Map
Satellite
Norwich
Great Yarmouth
Lowestoft
Thetford
Bury St Edmunds
Ipswich
Google
Map data ©2017 GeoBasis-DE/BKG (©2009), Google
Terms of Use
(CC-BY-SA) 2007-2017 Tamas Bartal | Questions and comments
Mirino | ECDL.web | Mars panoramas | GNewsTreemap.

Where am I?

Based on your **IP address**, we know the following about your location:

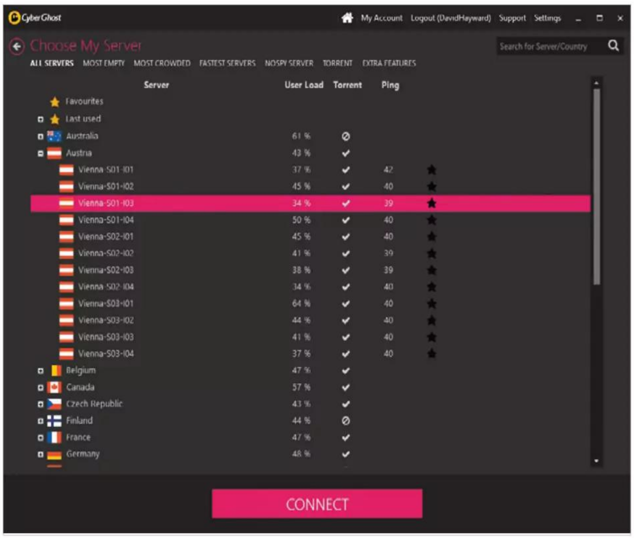
Country:
United Kingdom
City:
Lowestoft
Latitude:
N 52° 27' 7"
Longitude:
E 1° 41' 37"
Internet Service Provider:
BT
Organisation:
BT (British Telecommunications PLC)

STEP 8 Click back to the CyberGhost client and return to the main window. Click the Home icon along the top of the client window and then the Choose My Server button in the bottom right. This allows you to choose your own server from the available countries that CyberGhost works with.


CyberGhost
My Account
Logout (DavidHayward)
Support
Settings
Choose My Server
Search for Server/Country
ALL SERVERS
MOST EMPTY
MOST CROWDED
FASTEST SERVERS
NOSPY SERVER
TORRENT
EXTRA FEATURES

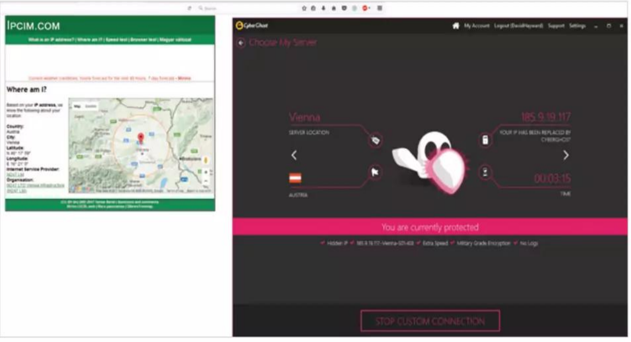
Server	User Load	Torrent	Ping
Favourites			
Last used			
Australia	61 %	⊘	
Austria	43 %	✓	
Belgium	47 %	✓	
Canada	57 %	✓	
Czech Republic	43 %	✓	
Finland	44 %	⊘	
France	47 %	✓	
Germany	48 %	✓	
Hong Kong	43 %	⊘	
Hungary	34 %	✓	
Iceland	32 %	⊘	
Israel	26 %	✓	
Italy	45 %	✓	
Japan	43 %	⊘	
Lithuania	50 %	⊘	
Luxembourg	43 %	✓	

STEP 9 Look through the list and pick a server; we're going to use one of the Vienna servers in this instance. The Ping value is how fast the server is, the lower the ping the faster the connection. Either click to highlight the server followed by clicking the Connect button or double-click to launch the server connection.


CyberGhost
My Account
Logout (DavidHayward)
Support
Settings
Choose My Server
Search for Server/Country
ALL SERVERS
MOST EMPTY
MOST CROWDED
FASTEST SERVERS
NOSPY SERVER
TORRENT
EXTRA FEATURES
CONNECT

Server	User Load	Torrent	Ping
Favourites			
Last used			
Australia	61 %	⊘	
Austria	43 %	✓	
Vienna-S01-I01	37 %	✓	42
Vienna-S01-I02	45 %	✓	40
Vienna-S01-I03	34 %	✓	39
Vienna-S01-I04	50 %	✓	40
Vienna-S02-I01	45 %	✓	40
Vienna-S02-I02	41 %	✓	39
Vienna-S02-I03	38 %	✓	39
Vienna-S02-I04	34 %	✓	40
Vienna-S03-I01	64 %	✓	40
Vienna-S03-I02	44 %	✓	40
Vienna-S03-I03	41 %	✓	40
Vienna-S03-I04	37 %	✓	40
Belgium	47 %	✓	
Canada	57 %	✓	
Czech Republic	43 %	✓	
Finland	44 %	⊘	
France	47 %	✓	
Germany	48 %	✓	

STEP 10 The CyberGhost client will take a few seconds to connect. When it's ready you'll see a 'You are currently protected' message in the client. Close your browser and relaunch it, then return to the www.ipcim.com/en/?p=where page. You can see that the Internet now thinks you're located where the chosen CyberGhost server is, protecting and securing your privacy and personal details.


IPCIM.COM
Where am I?
CyberGhost
Choose My Server
Vienna
SERVER LOCATION
AUSTRIA
185.9.19.117
YOUR IP HAS BEEN REPLACED BY CYBERGHOST
00:03:15
TIME
You are currently protected
STOP CUSTOM CONNECTION

Online Protection and Disaster Recovery

While you can successfully protect yourself and your own computer, as soon as you make a connection to the outside world you're under the influence of many external factors. We look at how data is transmitted from your computer to the Internet and how a canny hacker can intercept that data for their own means.

Over the coming pages you'll discover how best to protect yourself and what strategies you can use to become more secure when online; even when you're out and about with your Windows 10 laptop and other devices.

70 How Does Information Move Around the Internet?

72 How Can Internet Data be Intercepted?

74 10 Tips to Protect Yourself Against Interception

76 How to Secure Your Devices

78 How to Secure Yourself on Facebook

80 How to Secure Yourself on Twitter

82 How to Secure Yourself on WhatsApp

84 What to Avoid when Creating a Password

86 Password Generators and Tools

88 Top Ten Password Managers

90 Shopping Online and Security

92 How to Remove a Virus or Malware from a Windows PC

How Does Information Move Around the Internet?

Before we get into online protection and disaster recovery, it's worth taking a moment to look at how information moves around the Internet, in particular your information. Just how is data sent from your PC across the Internet, to potentially fall into the hands of someone else?

Information Superhighway

The Internet is a huge, complex network of computers and is widely credited as humanity's greatest achievement. It's estimated that the Internet houses something in the region of 10^{24} bytes of information, which is quite a lot.

That estimated 10^{24} bytes equates to an exabyte of potential information held by every single connected device that makes up the Internet, some of which is your information. It's an impossible number to visualise, since we're only using gigabytes or terabytes of storage in most of our devices. More to the point though, how on earth does all that connect together, and how does it work?

To be able to transmit all that information, the data that travels around the Internet is in packets. Each of these packets contains a header and a footer. The information stored in the header and footer contains the details regarding the data being sent. For example, if you send an email to someone, as soon as you click the send button the data will be wrapped up in headers and footers, split into numerous packets and sent on its merry way.

Whilst that sounds logical, much in the same way a telephone call takes place, the reality is quite different. Those packets can take any route possible to get to the destination, as defined by the header and footer. Those routes don't necessarily all have to be the same either. Some packets may travel from one server to the next via one data pathway, while others will take another. The server at the other end will use the information provided by the headers and footers to collate the message, reform the data and present it to the email recipient the way in which you intended it to.

Remarkably, if the server at the other end detects missing packets it can request the missing information from its available connections. Any missing data can then be sent via an alternative route, updating the information as it goes so other packets will know that the previous route isn't getting through. The headers and footers then tell the server that the data packets are all present and what they should look like; the email will arrive accordingly.

All this happens in milliseconds. This sounds incredibly complex and on paper it makes the Internet appear to be a slow, lumbering beast dealing with incomplete packets of data. In a way that's how it works but instead of being a lumbering beast, the Internet or more accurately, the servers and computers attached to it, are fathoming data packets by the millions every second.

Just as we've seen, each computer on the Internet is connected using an IP address. These are registered across the Internet, so the headers and footers in each packet contain the IP address of the sender and where the data is heading to. That way, it's not just a random collection of data travelling across the ether in the hope of landing in the right place. The DNS, Domain Name System, converts the IP addresses to readable names, such as Google.com and the like, and back again. That way when you enter the email address someone@somewhere.com the DNS servers will convert the information and the packets sent to the relevant destination.

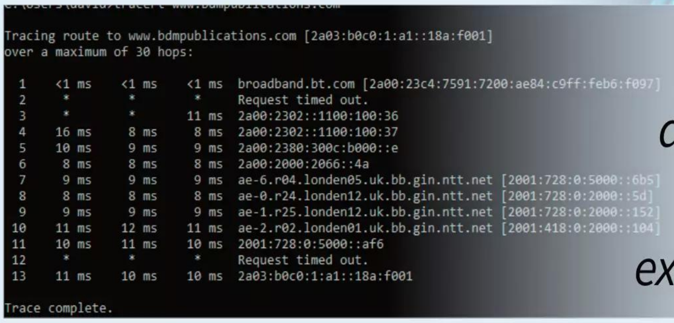
The protocols used throughout the Internet define what the data being communicated actually is. For example IMAP, Internet Message Access Protocol, is a mail protocol for accessing email on a remote server, such as accessing Gmail. These protocols help further the transmission of data to its intended location, making it more accurate and telling the computer on the other end what it is and how to piece together the jigsaw puzzle of packets that will be received.

Essentially this is how information is sent and received around the Internet. Obviously, there's a lot more going on in the background than we've mentioned here. The complexity that you can go into when dealing with data transfers is quite staggering and a little bewildering at times. Suffice to say, all those packets of data contain information about something or someone and somewhere out there are packets of data that contain information about you, where you are, what you're doing, and other personal details such as bank accounts, passwords, names and addresses.

> “*The Internet is regarded as the greatest human achievement, and it's not difficult to see why*”

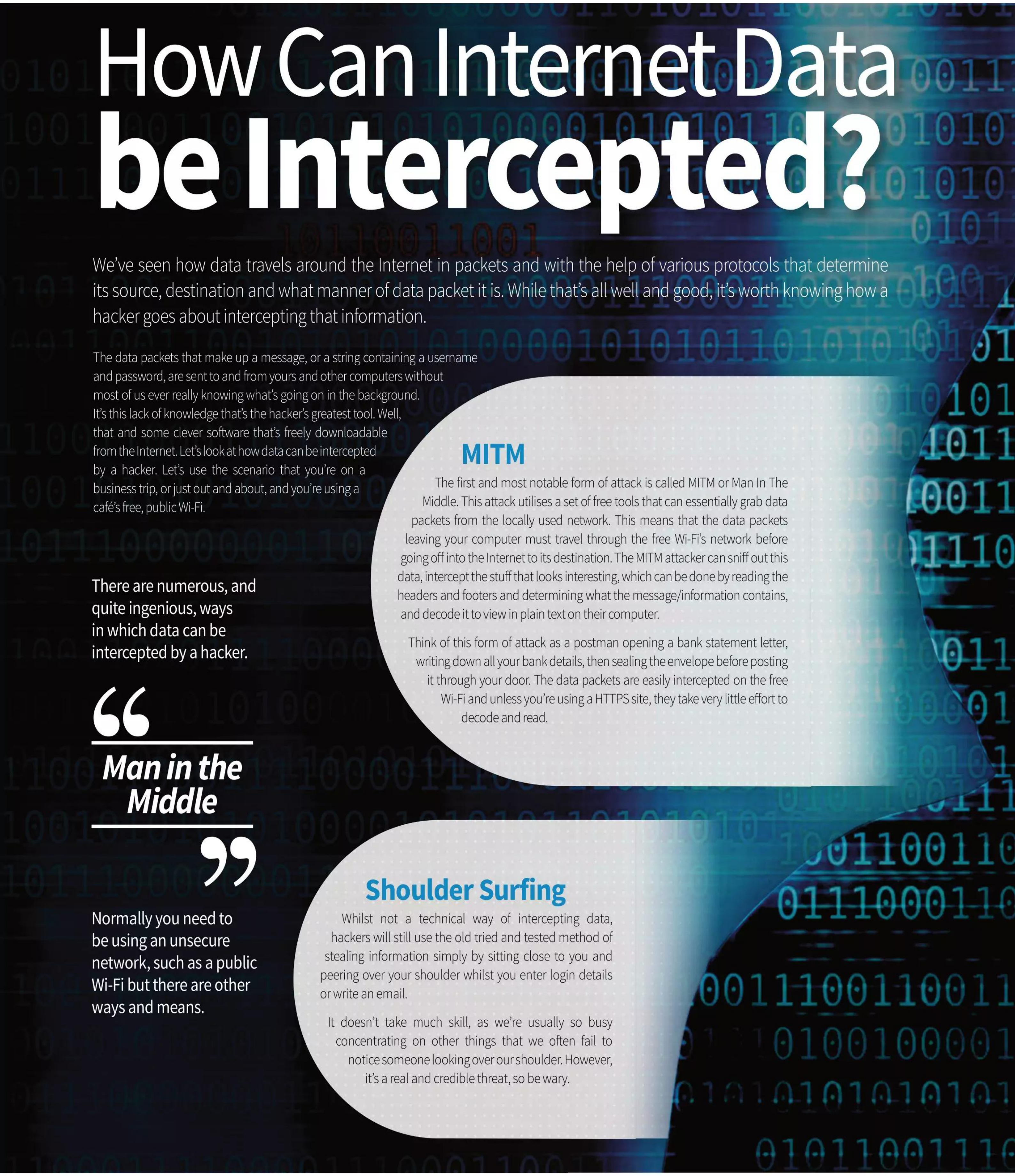
"Data is split into packets, with headers and footers telling servers what to do with it and where its going. "

"Along with protocols, packet information can take any possible route to its destination and it happens in a matter of milliseconds."



```
Tracing route to www.bdmpublications.com [2a03:b0c0:1:a1::18a:f001]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  broadband.bt.com [2a00:23c4:7591:7200:ae84:c9ff:feb6:f097]
  2     *        *        *     Request timed out.
  3     *        *       11 ms  2a00:2302::1100:100:36
  4    16 ms     8 ms     8 ms  2a00:2302::1100:100:37
  5    10 ms     9 ms     9 ms  2a00:2380:300c:b000::e
  6     8 ms     8 ms     8 ms  2a00:2000:2066::4a
  7     9 ms     9 ms     9 ms  ae-6.r04.londen05.uk.bb.gin.ntt.net [2001:728:0:5000::6b5]
  8     8 ms     8 ms     8 ms  ae-0.r24.londen12.uk.bb.gin.ntt.net [2001:728:0:2000::5d]
  9     9 ms     9 ms     9 ms  ae-1.r25.londen12.uk.bb.gin.ntt.net [2001:728:0:2000::152]
 10    11 ms    12 ms    11 ms  ae-2.r02.londen01.uk.bb.gin.ntt.net [2001:418:0:2000::104]
 11    10 ms    11 ms    10 ms  2001:728:0:5000::af6
 12     *        *        *     Request timed out.
 13    11 ms    10 ms    10 ms  2a03:b0c0:1:a1::18a:f001

Trace complete.
```

"DNS servers translate IP addresses to readable locations, the packets then know where exactly to head to deliver the data."



How Can Internet Data be Intercepted?

We've seen how data travels around the Internet in packets and with the help of various protocols that determine its source, destination and what manner of data packet it is. While that's all well and good, it's worth knowing how a hacker goes about intercepting that information.

The data packets that make up a message, or a string containing a username and password, are sent to and from yours and other computers without most of us ever really knowing what's going on in the background. It's this lack of knowledge that's the hacker's greatest tool. Well, that and some clever software that's freely downloadable from the Internet. Let's look at how data can be intercepted by a hacker. Let's use the scenario that you're on a business trip, or just out and about, and you're using a café's free, public Wi-Fi.

There are numerous, and quite ingenious, ways in which data can be intercepted by a hacker.

> “ *Man in the Middle* ”

Normally you need to be using an unsecure network, such as a public Wi-Fi but there are other ways and means.

MITM

The first and most notable form of attack is called MITM or Man In The Middle. This attack utilises a set of free tools that can essentially grab data packets from the locally used network. This means that the data packets leaving your computer must travel through the free Wi-Fi's network before going off into the Internet to its destination. The MITM attacker can sniff out this data, intercept the stuff that looks interesting, which can be done by reading the headers and footers and determining what the message/information contains, and decode it to view in plain text on their computer.

Think of this form of attack as a postman opening a bank statement letter, writing down all your bank details, then sealing the envelope before posting it through your door. The data packets are easily intercepted on the free Wi-Fi and unless you're using a HTTPS site, they take very little effort to decode and read.

Shoulder Surfing

Whilst not a technical way of intercepting data, hackers will still use the old tried and tested method of stealing information simply by sitting close to you and peering over your shoulder whilst you enter login details or write an email.

It doesn't take much skill, as we're usually so busy concentrating on other things that we often fail to notice someone looking over our shoulder. However, it's a real and credible threat, so be wary.

Fake Wi-Fi

This is another element to a MITM attack, also known as an Evil Twin. Essentially a hacker can sit at the same café as you and everyone else and use a set of tools that can pretend to be the actual Wi-Fi router belonging to the café. This enables them to do several things: first, they're able to beam out the fake Wi-Fi signal to every device within range, which in turn (if the users have their devices set to attach to any freely available Wi-Fi) will instantly connect to the fake signal. Secondly, once they have a device connected, they're able to use their laptop and the tools therein to intercept all the traffic that's being sent to their fake Wi-Fi signal. Thirdly, the attacker can connect themselves to the actual café Wi-Fi and act as a filter to the real connection to the Internet. The victim isn't even aware that their connection is compromised.

Naturally, this means that every single scrap of data is being filtered through the hacker's system. It's just up to them to collect it all, decode it and use the information within for their own gains.

Fake Sites

We've mentioned fake websites previously. This way of data interception is often working hand-in-hand with the scenario we're using as an example. Combining the aforementioned Evil Twin and packet sniffing methods, a hacker, who has taken the time to set up the scam, can create several fake website front ends that mimic banking sites, Outlook access, login pages and so on. They then host those sites on their interception laptop, together with the Evil Twin fake Wi-Fi and should a user connect and request the page of their bank they instead get the fake site that the hacker set up.

The victim will then unwittingly enter their details, which will be stored by the hacker before forwarding the victim to the actual bank website. The victim will then be required to re-enter their banking details into the actual bank website. For their part, they simply think they're mistyped a password and gain access to their account as normal. Sadly, the hacker now has plain text information regarding all their login details and can begin to transfer money from their account.

10 Tips to Protect Yourself Against Interception

While it may seem like fearmongering, detailing the ways in which data can be intercepted, it's sadly a real world fact. Public Wi-Fi, hotspots and free access points are the bane of the security industry. Thankfully, there are ways in which you can protect yourself.

Public Safety

Despite the different and varied ways a hacker can gain access to your inbound and outbound data, there are means in which you can defend yourself. Here are ten tips to help you protect your data from being intercepted.

TIP 1 Not all public Wi-Fi access points are havens for nefarious hackers but that doesn't mean you should let your guard down. Every security software and firewall in the world can't help you if you're not savvy when it comes to information security. If you're going to use public Wi-Fi, don't use it for banking or other highly personal detail transactions.

Online Banking

TIP 2 It may not always be possible to spot an Evil Twin fake Wi-Fi access point. It's often best to double-check with members of staff, if it's a café, airport, restaurant or similar, that the Wi-Fi you're connecting to is actually theirs and not one that's being spoofed. Avoid Wi-Fi names like 'Free Wi-Fi Here' or similar.

TIP 3 Always double-check a website for spelling errors, older logos or anything else that may raise an alarm. If your banking website looks even remotely different from when you last used it, try and avoid logging into it until you get to a more secure Internet location.

TIP 4 Ensure you use the latest antivirus and antimalware definitions for your security client. If you're going to use public Wi-Fi, make sure you're up to date prior to leaving, especially airport Wi-Fi points, and that the client is in good working order.

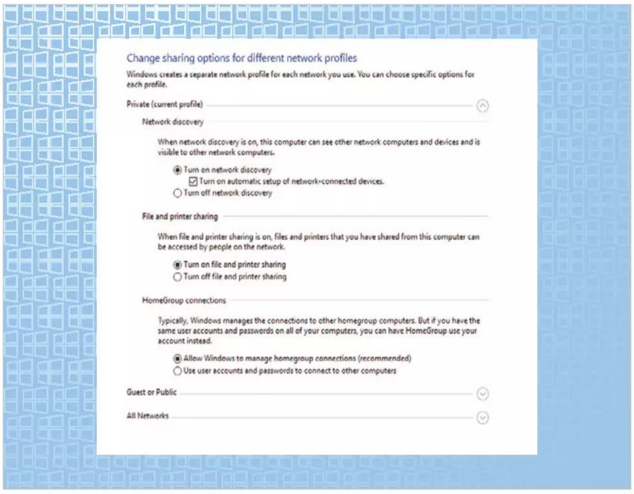
backspace
delete
online banking
shift

TIP 5

Always use HTTPS to access any website. This means that the information and data packets will be sent and received in an encrypted form and will make it exceedingly difficult for a hacker to decipher them. If possible, use an add-on such as HTTPS Everywhere for your browser of choice.

TIP 6

Turn off file sharing when you're using a public Wi-Fi access point. Whilst it's great to share your content on your home or work network, once you start using another network, your computer could start sharing that data with anyone who's also connected to the same network.



Change sharing options for different network profiles

Windows creates a separate network profile for each network you use. You can choose specific options for each profile.

Private (current profile)

Network discovery

When network discovery is on, this computer can see other network computers and devices and is visible to other network computers.

● Turn on network discovery
☑ Turn on automatic setup of network-connected devices.
○ Turn off network discovery

File and printer sharing

When file and printer sharing is on, files and printers that you have shared from this computer can be accessed by people on the network.

● Turn on file and printer sharing
○ Turn off file and printer sharing

HomeGroup connections

Typically, Windows manages the connections to other homegroup computers. But if you have the same user accounts and passwords on all of your computers, you can have HomeGroup use your account instead.

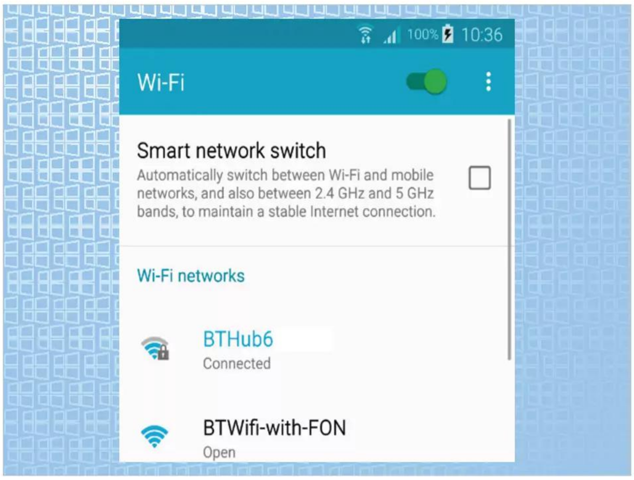
● Allow Windows to manage homegroup connections (recommended)
○ Use user accounts and passwords to connect to other computers

Guest or Public

All Networks

TIP 7

If you're not planning on using any public Wi-Fi points, then make sure that the Wi-Fi is turned off on your laptop, phone, tablet and other devices you have on you. There are instances when a device can automatically attach to any available network, unless otherwise told not to.



Smart network switch
Automatically switch between Wi-Fi and mobile networks, and also between 2.4 GHz and 5 GHz bands, to maintain a stable Internet connection. ☐

Wi-Fi networks

BTHub6
Connected

BTWifi-with-FON
Open

TIP 8

Using a VPN when accessing a public Wi-Fi point is a fantastic way of protecting your data packets. They can still be intercepted but the VPN client encrypts all outgoing and incoming data with the highest possible levels, making it virtually impossible for a hacker to decode.

TIP 9

To avoid shoulder surfers, make sure that the area behind you is clear and enter passwords etc. via your keyboard in the same way you'd protect your card details in an ATM. Cover your keyboard as much as possible and make a point of looking around to make sure no one is watching you over your shoulder.

TIP 10

If possible, always use a two-factor form of authentication. For example, some banks will utilise both a login from their website as well as a text sent with a unique code to a registered phone number. This way you ensure that the banking site is legitimate and a hacker can't go any further without the SMS pin sent by the bank.

How to Secure Your Devices

Mobile device hacking is on the rise. Most people now carry a phone or tablet around with them all the time, containing their emails, browser data, photos and enough personal information for someone to be interested.

Ten Tips for Safer Mobiles

Your personal information is worth quite a bit to the right group of people. It's not just Windows 10 security you need to keep in mind, you need to consider your mobile security too.

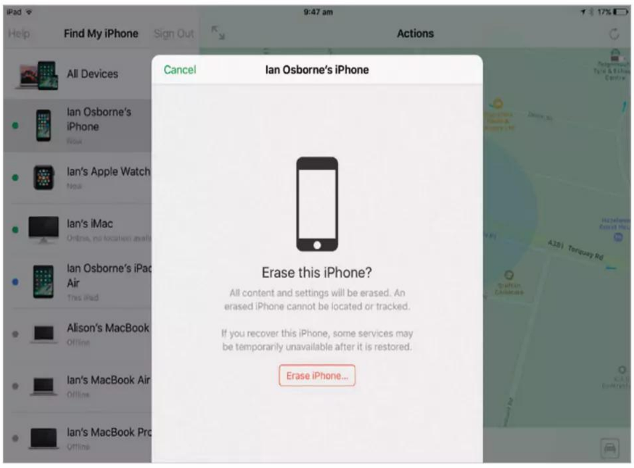
SECURITY LOCK

Locking your device is one of the most basic of security tips for mobile devices. Either use a number code, pattern lock or finger print to lock your device when not in use. Should someone steal it, it becomes a little more difficult for them to gain access. That won't stop a professional digital criminal, but it will deter the rest.

dtac
Touch ID or Enter Passcode
1
2 ABC
3 DEF
4 GHI
5 JKL
7 PQRS
8 TUV
9 WXYZ
0
Emergency
Delete

REMOTE WIPE

If possible set up some form of remote wipe. Should your phone or tablet be stolen or lost, you'll be able to use another Internet connected computer to send a delete signal to the lost device. You may never see the phone again but at least the personal data within is now out of the hands of others.


iPad
9:47 am
17%
Help
Find My iPhone
Sign Out
Actions
All Devices
Ian Osborne's iPhone
Ian's Apple Watch
Ian's iMac
Ian Osborne's iPad Air
Alison's MacBook
Offline
Ian's MacBook Air
Offline
Ian's MacBook Pro
Offline
A381 Torquay Rd

Cancel
Ian Osborne's iPhone

Erase this iPhone?

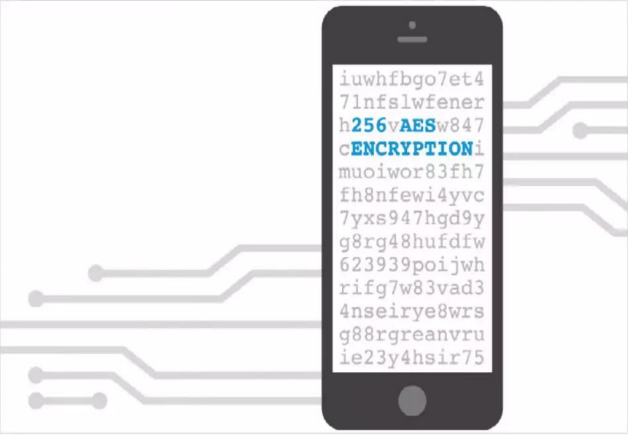
All content and settings will be erased. An erased iPhone cannot be located or tracked.

If you recover this iPhone, some services may be temporarily unavailable after it is restored.

Erase iPhone...

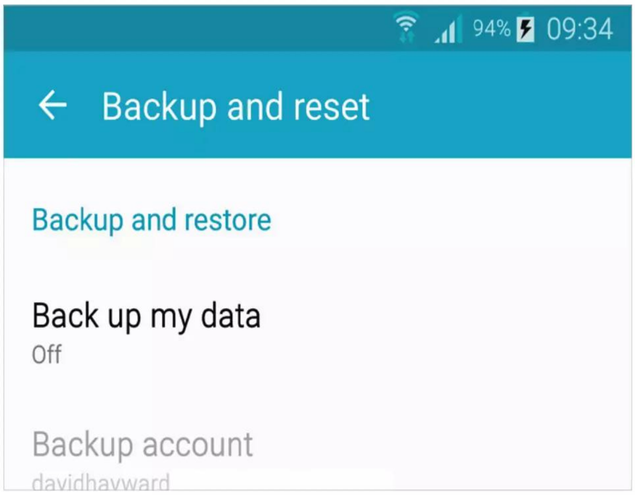
MOBILE ENCRYPTION

It's possible to set up data encryption on mobile devices these days. For example, you can encrypt the entire device or just the part that contains emails and personal or banking data. Either way, encryption will protect the contents of your device.


iuwhfbgo7et4
71nfslwfener
h256vAESw847
cENCRYPTIONi
muoiwor83fh7
fh8nfewi4yvc
7yxs947hgd9y
g8rg48hufdfw
623939poijwh
rifg7w83vad3
4nseirye8wrs
g88rgreanvru
ie23y4hsir75

BACKUP DATA

Make sure that the data you have on your device is regularly backed up. You may have umpteen security elements in place but if the device is lost and you haven't made a backup, then your data is lost too.



Backup and reset

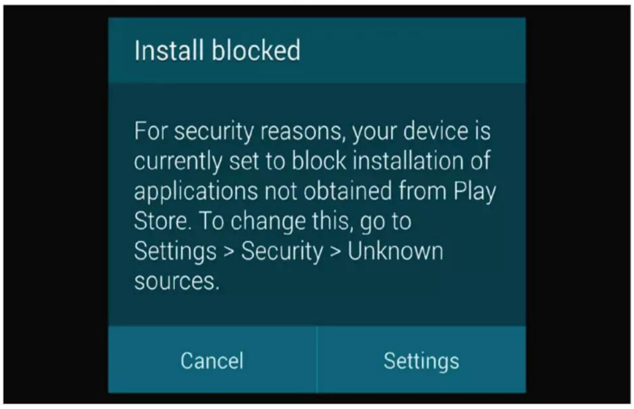
Backup and restore

Back up my data
Off

Backup account
davidhayward

BLOCK INSTALLATIONS

Try to avoid installing third-party apps. iOS devices are covered in this regard thanks to Apple's walled garden approach to its app store. However, Android users are particularly vulnerable. Don't install anything from an unknown source and research plenty before installing anything.



Install blocked

For security reasons, your device is currently set to block installation of applications not obtained from Play Store. To change this, go to Settings > Security > Unknown sources.

Cancel
Settings

NO ROOTING

Avoid jailbreaking or rooting your device. Whilst it's regarded as a positive process, to remove the built-in software from the manufacturer and give you control over the device, it often also opens your device to backdoors that were previously sealed. Unless you know how to properly secure a device, leave rooting alone.

UPDATE SYSTEM

Keep your system as up to date as possible. It can be a pain having to frequently accept update and upgrade messages from your device, and waiting for the OS or the app to update itself, but more often than not an update will provide much needed security patches.

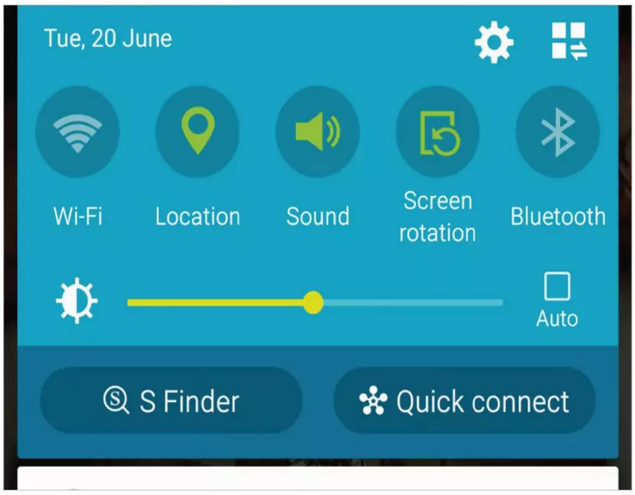
htc
SETTINGS
11:22
phone update
Update status
Downloading updates 17%
Tell me when updates are available for my phone
Automatically d
data se

FALSE TEXTS

Be aware of social engineering phone scams, Vishing and Smishing in particular. Criminals love sending false banking texts, links to fake websites and all manner of other scams designed to gain access to your personal information.

POWER OFF WI-FI

Remember to turn off your Wi-Fi when you leave the home or office network. If you desperately require Internet access and don't want the data charges, then consider using a VPN if you're connecting to public Wi-Fi points.


Tue, 20 June
Wi-Fi
Location
Sound
Screen rotation
Bluetooth
Auto
S Finder
Quick connect

MOBILE AV

Download and install a good mobile antivirus and malware tool set. Bitdefender, McAfee and all the other major security companies offer a mobile version of their products and with it you'll be better prepared for any potential cyber attack.

Bitdefender Mobile Security
Your device is safe
Last scan: Two weeks ago
Malware Scanner
Anti-theft
Web Security
Security
Event Viewer

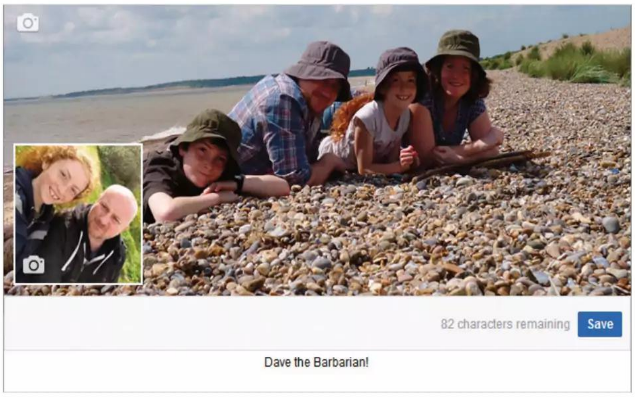
How to Secure Yourself on Facebook

Facebook has become one of the best sources for cyber criminals to gain personal information on the Internet. Without realising it, a user is giving out reams of data and in most circumstances they're making it public.

Tips for Better Facebook Profiles

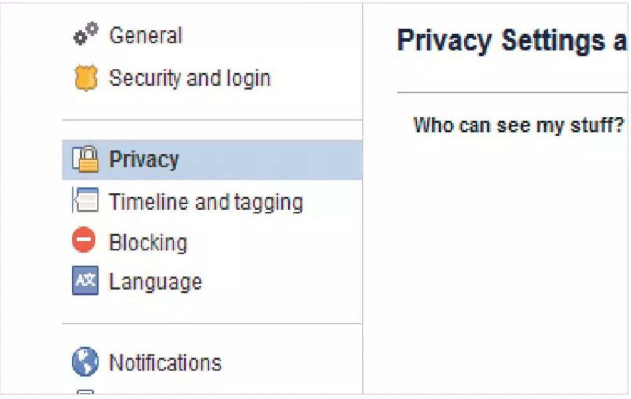
The dangers of social media aren't just for young people, many adults have been duped into befriending someone they don't know and exposing their personal information.

Facebook's policy forbids the use of fake names but it does allow nick names to be used. Where possible, use your nickname instead of your real name. This will effectively hide your real name details from those who would wish to exploit it.



Dave the Barbarian!

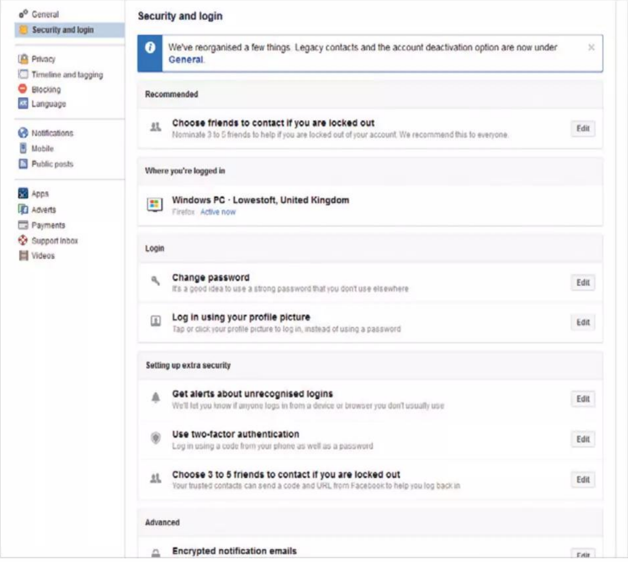
Go to Settings > Privacy, and make sure that the Who can see my stuff section is set for just friends, as opposed to friends of friends or public. This will effectively hide your Timeline contents from others and only your confirmed friends will be able to see any updates.



Privacy Settings a

Who can see my stuff?

Set up two-factor authentication, alerts about unrecognised logins and make sure that emails from Facebook are encrypted. These can all be found in the Settings > Security and Login section.



Security and login

We've reorganised a few things. Legacy contacts and the account deactivation option are now under General.

Recommended

Choose friends to contact if you are locked out
Nominate 3 to 5 friends to help if you are locked out of your account. We recommend this to everyone.

Where you're logged in

Windows PC · Lowestoft, United Kingdom
Firefox · Active now

Login

Change password
It's a good idea to use a strong password that you don't use elsewhere

Log in using your profile picture
Tap or click your profile picture to log in, instead of using a password

Setting up extra security

Get alerts about unrecognised logins
We'll let you know if anyone logs in from a device or browser you don't usually use

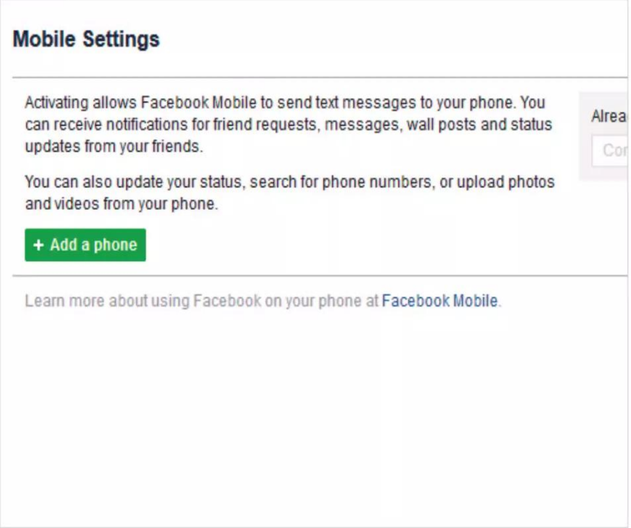
Use two-factor authentication
Log in using a code from your phone as well as a password

Choose 3 to 5 friends to contact if you are locked out
Your trusted contacts can send a code and URL from Facebook to help you log back in

Advanced

Encrypted notification emails

Never post any contact information on your profile. We often automatically start filling in the phone number field on a site but take a moment to consider what the ramifications could be should your number be made aware outside your circle of friends. That also includes house address too.



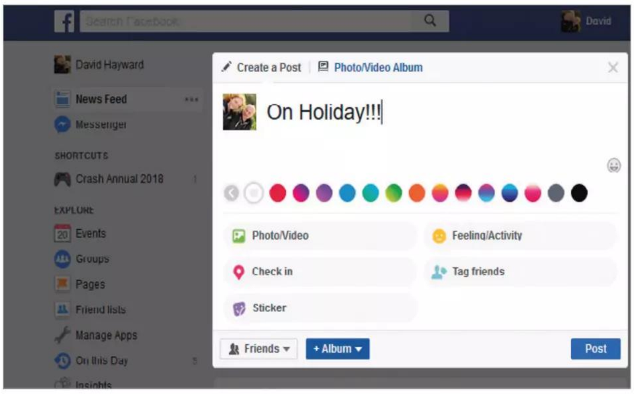
Mobile Settings

Activating allows Facebook Mobile to send text messages to your phone. You can receive notifications for friend requests, messages, wall posts and status updates from your friends.

You can also update your status, search for phone numbers, or upload photos and videos from your phone.

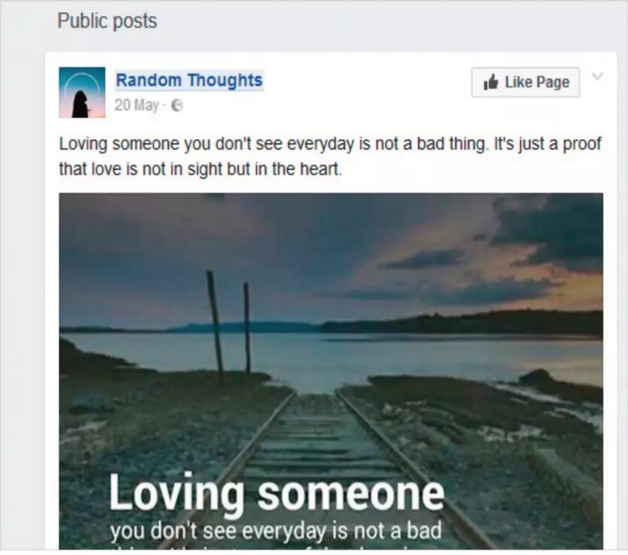
Learn more about using Facebook on your phone at Facebook Mobile.

Tempting as it may be, try to avoid posting your location. Whether you're at home alone, or you're on holiday, should that information be made available then a criminal will know that your house is empty or worse, that you're alone in it.


Search Facebook
David
David Hayward
News Feed
Messenger
SHORTCUTS
Crash Annual 2018
EXPLORE
Events
Groups
Pages
Friend lists
Manage Apps
On this Day
Insights
Create a Post
Photo/Video Album
Photo/Video
Feeling/Activity
Check in
Tag friends
Sticker
Friends
+ Album
Post

On Holiday!!!

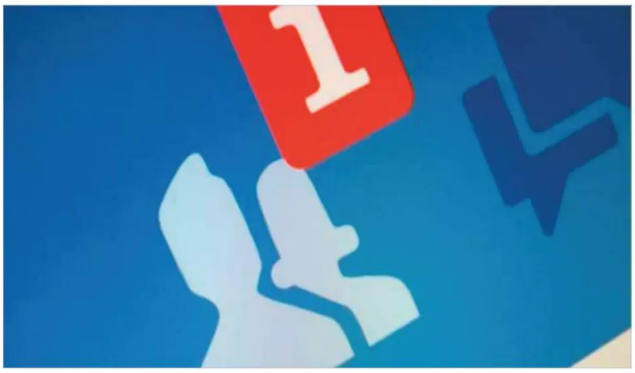
Try and avoid sharing random thoughts of the day, inspirational quotes, fake news or other such items that appear on your Timeline from others. Often these instances are created to farm for shares and likes and as such can often be traced back to individuals who are simply looking for active Facebook accounts.


Public posts
Like Page
Loving someone
you don't see everyday is not a bad

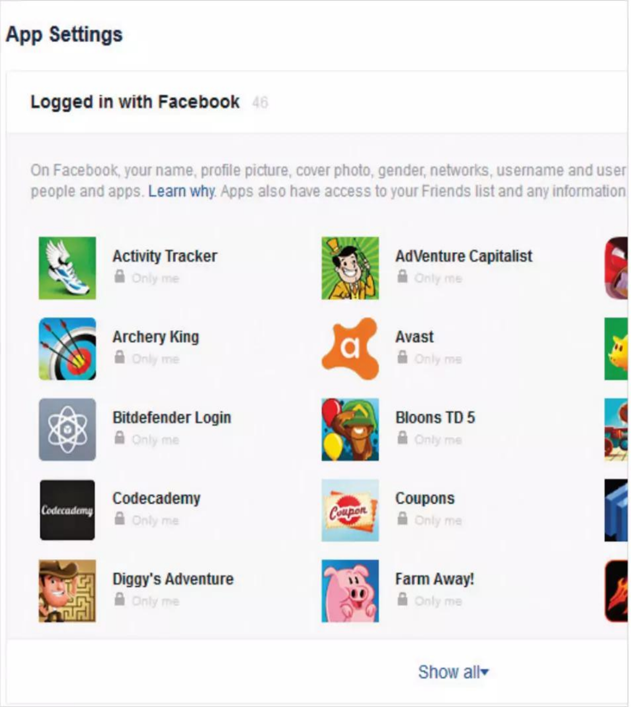
Random Thoughts
20 May ·

Loving someone you don't see everyday is not a bad thing. It's just a proof that love is not in sight but in the heart.

Try not to accept every friend request you get. Take a moment to check the person out and if necessary message them to find out who they are and how they know you. If their comment is something like 'we met at the bar last month' then it's best to ignore the request, as they could be fishing for information.



Not all apps you install on your phone or tablet are good. Take a moment to read what an app will try to access when it's installed. Often a rogue app will attempt to access your Facebook account to farm for your and your friend's information.



App Settings

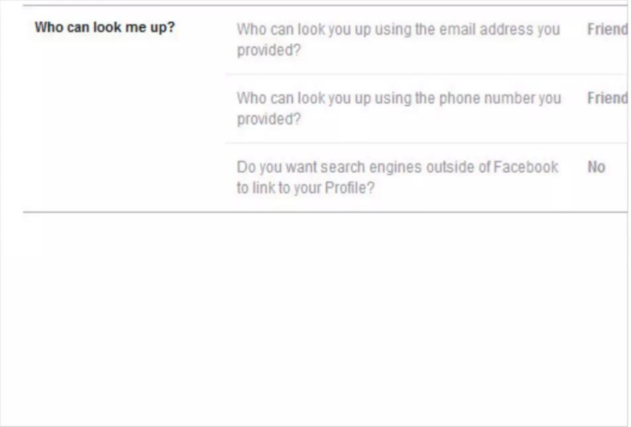
Logged in with Facebook 46

On Facebook, your name, profile picture, cover photo, gender, networks, username and user
people and apps. Learn why. Apps also have access to your Friends list and any information

Activity Tracker Only me	**AdVenture Capitalist** Only me
Archery King Only me	**Avast** Only me
Bitdefender Login Only me	**Bloons TD 5** Only me
Codecademy Only me	**Coupons** Only me
Diggy's Adventure Only me	**Farm Away!** Only me

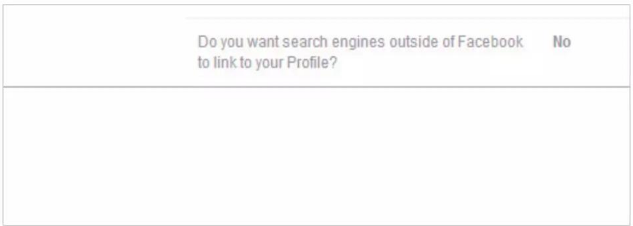
Show all▾

Whilst in the Settings > Privacy section, consider editing the default options for the Who can look me up fields. These will prevent the public, or even friends of friends, from being able to find you on Facebook, which in turn adds a higher level of security to your account.



Who can look me up?	Who can look you up using the email address you provided?	Friend
	Who can look you up using the phone number you provided?	Friend
	Do you want search engines outside of Facebook to link to your Profile?	No

Finally, ensure that the Do you want search engines outside of Facebook to link to your profile option is set to No. This will hide you from someone who has entered your name into Google in the hope that they might be able to find your Facebook account.



Do you want search engines outside of Facebook to link to your Profile? No

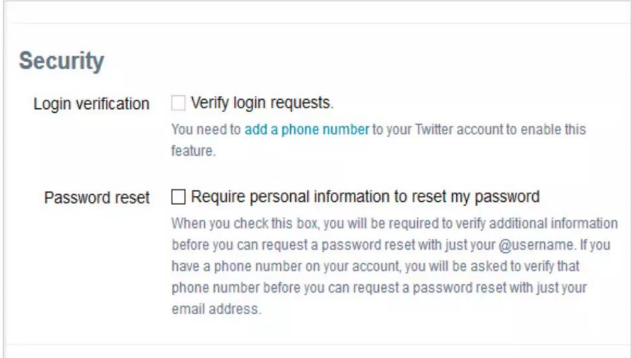
How to Secure Yourself on Twitter

Twitter's success has boomed in recent years. Where once it was simply one of the more popular social media platforms, thanks to presidential candidates and scores of celebrities, it's fast become the modern media phenomenon.

Securing the Twitterverse

Sadly, due to its popularity, Twitter is a hotbed of scammers, spammers, hackers and social engineers scouting out the next potential victim for monetary gain, or simply behaving abusively. Here are ten tips to help secure your Twitter account.

If you click on your profile picture and choose Settings and Privacy from the menu, you're able to set up a form of two-factor authentication called Verify Login Requests. This will enable Twitter to use your phone number to send texts for any login requests. So even if your password is compromised, the hacker can't get in without the text code.



Security

Login verification ☐ Verify login requests.
You need to add a phone number to your Twitter account to enable this feature.

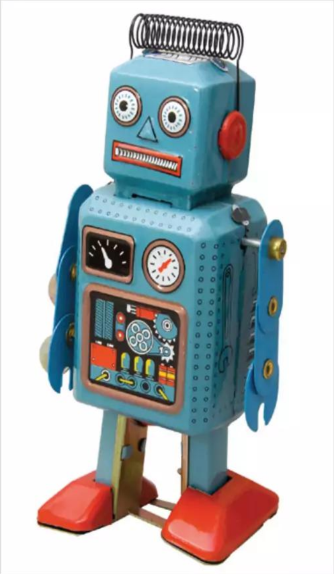
Password reset ☐ Require personal information to reset my password
When you check this box, you will be required to verify additional information before you can request a password reset with just your @username. If you have a phone number on your account, you will be asked to verify that phone number before you can request a password reset with just your email address.

Just like most other social media platforms, phishing scams are rife on Twitter. Be wary of anyone sending you Tweets claiming to be someone you know, offering a too-good-to-be-true job or even informing you that your account is compromised. It's likely a phishing scam, so delete and report the instance to Twitter.

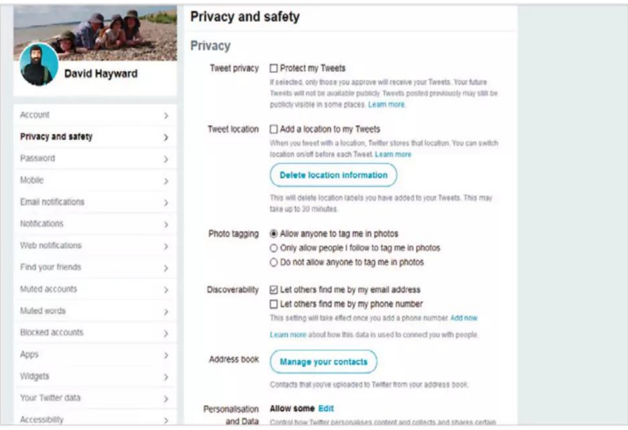
USERNAME:
PASSWORD:

We've previously mentioned the fact that using weak passwords is, unsurprisingly, not recommended. However, you'd be amazed at how many people still use the likes of 'password1234' or something similar. Set a good, strong password that will take some cracking.

There are many accounts on Twitter that simply aren't real. These bots, as they're known, can be programmed to post daily amusing, inspiring and socially acceptable Tweets. On the flip side, other bots are designed to Tweet suspicious links to virus-infested websites. In short, unless you trust the account, don't follow any links.address too.



Within your account settings, you'll see a menu to the left with a Privacy and Safety option. Click this to enable Twitter privacy, Discoverability, Direct Message notifications, the ability to hide sensitive Tweets and the removal of blocked accounts. It's worth going through the list to further secure your account.



David Hayward

- Account
- **Privacy and safety**
- Password
- Mobile
- Email notifications
- Notifications
- Web notifications
- Find your friends
- Muted accounts
- Muted words
- Blocked accounts
- Apps
- Widgets
- Your Twitter data
- Accessibility

Privacy and safety

Privacy

Tweet privacy: ☐ Protect my Tweets
If selected, only those you approve will receive your Tweets. Your future Tweets will not be available publicly. Tweets posted previously may still be publicly visible in some places. Learn more

Tweet location: ☐ Add a location to my Tweets
When you tweet with a location, Twitter stores that location. You can switch location on/off before each Tweet. Learn more
Delete location information
This will delete location labels you have added to your Tweets. This may take up to 30 minutes.

Photo tagging:
● Allow anyone to tag me in photos
○ Only allow people I follow to tag me in photos
○ Do not allow anyone to tag me in photos

Discoverability:
☑ Let others find me by my email address
☐ Let others find me by my phone number
This setting will take effect once you add a phone number. Add now
Learn more about how this data is used to connect you with people.

Address book: Manage your contacts
Contacts that you've uploaded to Twitter from your address book.

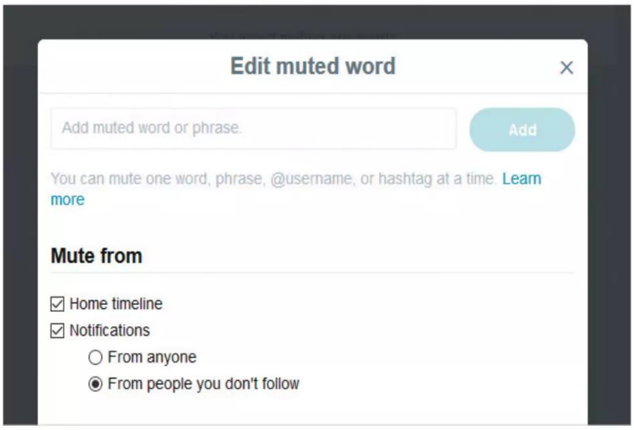
Personalisation and Data: **Allow some** Edit
Control how Twitter personalises content and collects and shares certain

Direct messaging in Twitter is both advantageous and dangerous at the same time. Whilst great for communicating directly with another user, it's also used by others to lure in victims or send links to malicious websites. It's best to ignore most messages unless you know who they're from.

If you use your Twitter account to login into any third-party apps or games, then you may need to consider setting up a secondary Twitter account. Whilst convenient, some apps can be hijacked to collect account details, leaking them to hackers.

Facebook
Twitter

Word Muting is an excellent feature within Twitter's account settings. With it you're able to mute any words you don't want to see in your notifications or timeline. There are often Tweets you'd like to avoid even seeing in your timeline, so muting them is an ideal solution to help keep your account clean and free from negative aspects.



Edit muted word

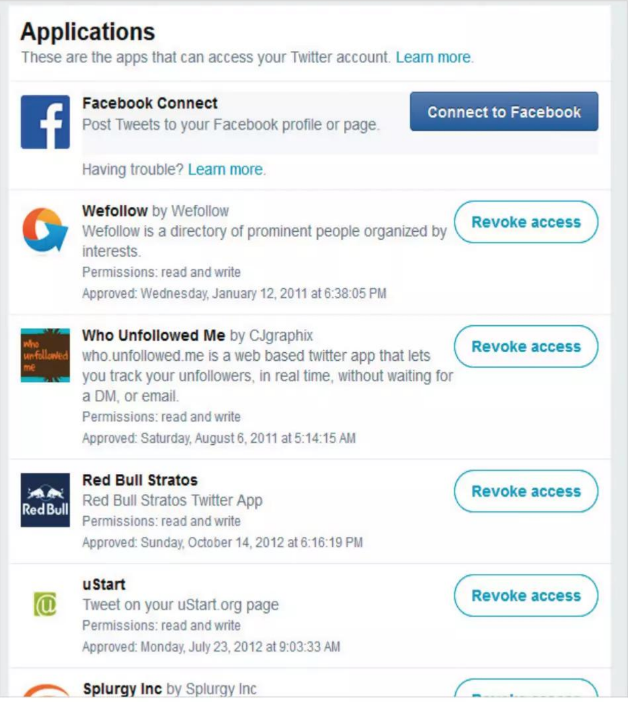
Add muted word or phrase. Add

You can mute one word, phrase, @username, or hashtag at a time. Learn more

Mute from

☑ Home timeline
☑ Notifications
○ From anyone
● From people you don't follow

It's always worth browsing through the Apps section in the Twitter options. This is where you can allow or revoke access for any apps you've used via the Twitter account; and you can also see what rights each app has to your Twitter account.



Applications

These are the apps that can access your Twitter account. Learn more.

Facebook Connect
Post Tweets to your Facebook profile or page.
Connect to Facebook
Having trouble? Learn more.

Wefollow by Wefollow
Wefollow is a directory of prominent people organized by interests.
Permissions: read and write
Approved: Wednesday, January 12, 2011 at 6:38:05 PM
Revoke access

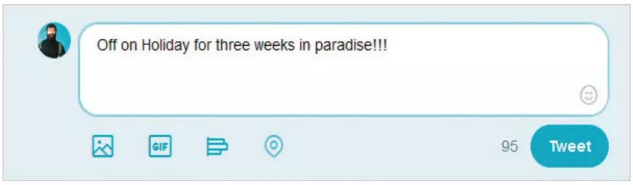
Who Unfollowed Me by CJgraphix
who.unfollowed.me is a web based twitter app that lets you track your unfollowers, in real time, without waiting for a DM, or email.
Permissions: read and write
Approved: Saturday, August 6, 2011 at 5:14:15 AM
Revoke access

Red Bull Stratos
Red Bull Stratos Twitter App
Permissions: read and write
Approved: Sunday, October 14, 2012 at 6:16:19 PM
Revoke access

uStart
Tweet on your uStart.org page
Permissions: read and write
Approved: Monday, July 23, 2012 at 9:03:33 AM
Revoke access

Splurgy Inc by Splurgy Inc

Like Facebook, be careful of what you post. It's nice letting others know you're off on holiday to the Bahamas for several weeks but there could be a rogue account that's now informed of an empty house; and if you were foolish enough to mention your address in previous Tweets, they know exactly where to go.



Off on Holiday for three weeks in paradise!!!

95 Tweet

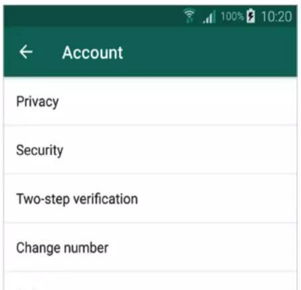
How to Secure Yourself on WhatsApp

With over a billion users worldwide, WhatsApp is proving to be a force to be reckoned with in the social media marketplace. This messaging app was released over eight years ago and developed by the Facebook team; since then it's become the most popular messaging app.

WhatsApp Security Tips

With this popularity comes a darker side to messaging. Accounts of terrorists using WhatsApp, along with hackers, scammers and all manner of nefarious individuals and groups are ever in the popular media.

Protecting your WhatsApp account can be done mainly through the Settings > Account > Privacy option. In here you're able to secure your personal details, profile, status, messaging and who can see your account.


100% 10:20

Account

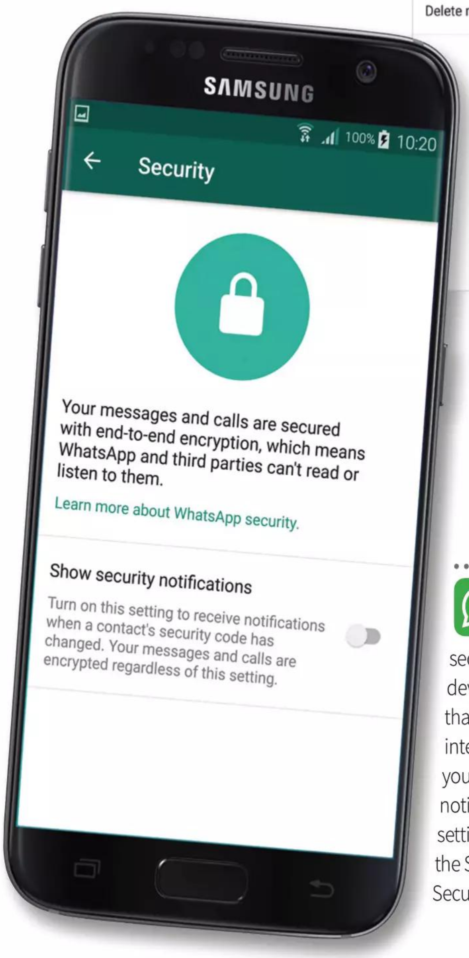
Privacy

Security

Two-step verification

Change number

Delete my account



Security

Your messages and calls are secured with end-to-end encryption, which means WhatsApp and third parties can't read or listen to them.

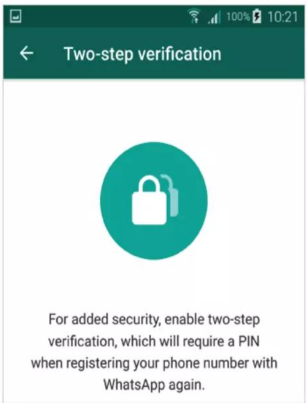
Learn more about WhatsApp security.

Show security notifications

Turn on this setting to receive notifications when a contact's security code has changed. Your messages and calls are encrypted regardless of this setting.

Thankfully, WhatsApp already encrypts and secures messages sent from one device to another. This means that your data can't be intercepted and read. However, you can opt to view security notifications if a contact's security setting has been altered. This is in the Settings > Account > Security menu.

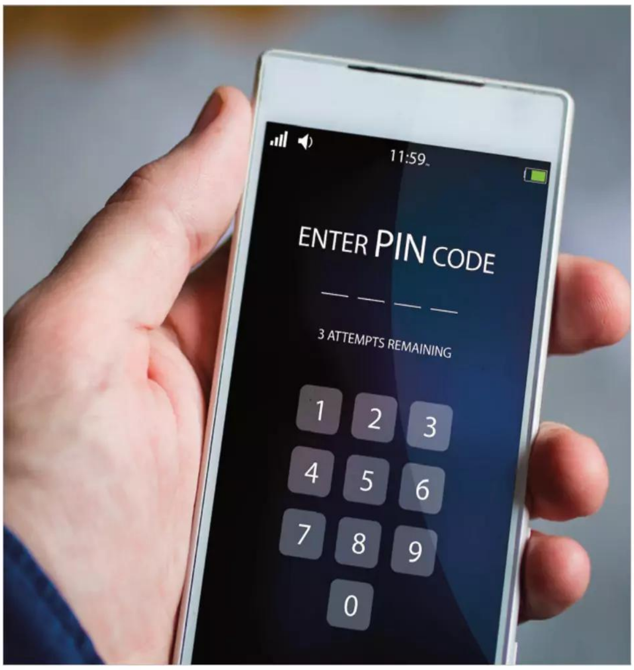
For added security you can opt for two-step authentication, which will require a PIN when registering your phone number with WhatsApp. This is an absolute must for those who use the app regularly.


100% 10:21

Two-step verification

For added security, enable two-step verification, which will require a PIN when registering your phone number with WhatsApp again.

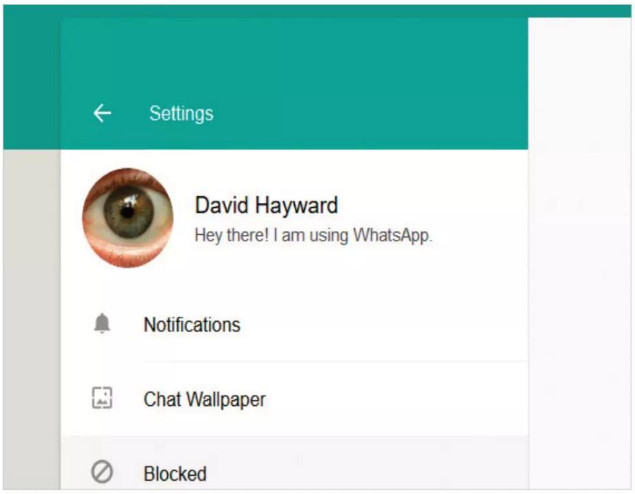
Beyond WhatsApp itself, make sure that your phone or tablet is securely locked with an access PIN, pattern, facial or finger print recognition system. This way, should you lose your phone, it will be locked against anyone who tries to access it and WhatsApp.



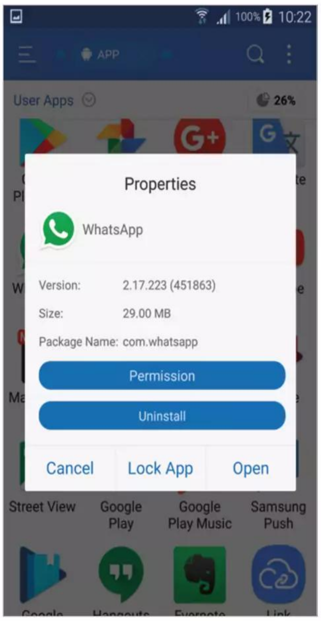
Generally you're not able to add users to your chat list if you don't already have them in your contacts list. However, clever phishing scams can have a victim add a contact, who can then message them using WhatsApp; as with all social media platforms, be wary of phishing attacks.

http:\\ Your. Bank
Password?

You can block users via the WhatsApp Web feature. Log into WhatsApp Web, and click on the three horizontal dots by your profile picture. Then click Settings and from there the Blocked option. You can select contacts to block from WhatsApp.

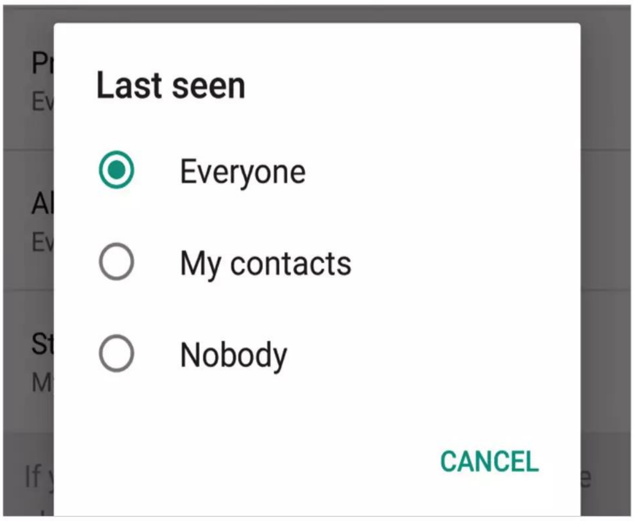

Settings
David Hayward
Hey there! I am using WhatsApp.
Notifications
Chat Wallpaper
Blocked

You can block all images from appearing on your photostream within WhatsApp. iOS users can look to their Settings then Privacy > Photos and deselect WhatsApp from the list of allowed apps. Android users will need to create a file called .nomedia within the WhatsApp images folder to stop the app from listing pictures.


100% 10:22
APP
User Apps
26%
Properties
WhatsApp
Permission
Uninstall
Cancel
Lock App
Open
Street View
Google Play
Google Play Music
Samsung Push

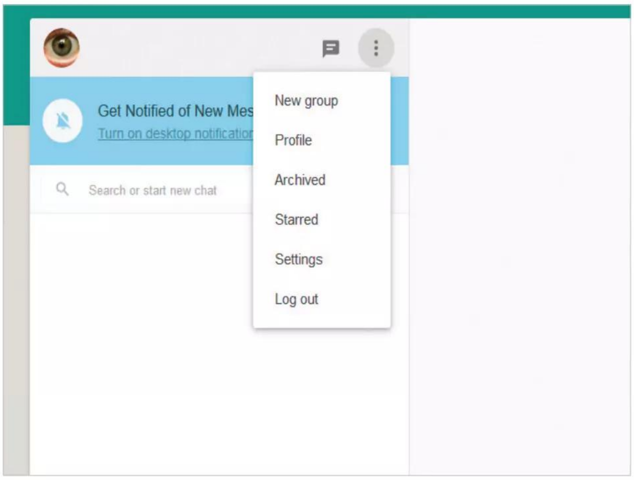
Version: 2.17.223 (451863)
Size: 29.00 MB
Package Name: com.whatsapp

If you don't want WhatsApp contacts to see where you've been, you need to disable the Last Seen option within the Privacy settings. This will prevent other users from 'seeing' your movements. Should a malicious contact be added, they will never know where you are or have been.


Last seen
● Everyone
○ My contacts
○ Nobody
CANCEL

Be wary of scams where you're contacted through other social media accounts informing you that your WhatsApp account has been compromised. These often request you to add a so-called legitimate contact, who in reality isn't, or visit a webpage that's riddled with malware.

If you use WhatsApp Web it's always best to ensure that you've logged out of it correctly before leaving your computer. The last thing you need is for someone to come over to your computer and view any conversations between contacts.


Get Notified of New Mes
Turn on desktop notification
Search or start new chat
New group
Profile
Archived
Starred
Settings
Log out

What to Avoid when Creating a Password

Creating a strong password sounds easy on paper but when you're presented with the password box it's easy to become stumped. Should you get past that part, there are also security rules to follow to further protect that password.

PA55W0RD1234

To help you create the perfect password, and secure it further, here are ten tips for happier password management. There's always password pitfalls but stick to these general tips and you should be okay.

OBVIOUS DATES

Never use your date of birth, partner's date of birth, children's date of birth, pet's names, family names or even the town where you grew up in. This is all information that can easily be collected from social media sites or even a clever Internet search.

BAD
PASSWORD

SAME PASSWORDS

Never use the same password for multiple sites. It's tempting and easy to have a single password for everything but should that password ever become compromised you will lose access to every site you visit, including any banking sites.

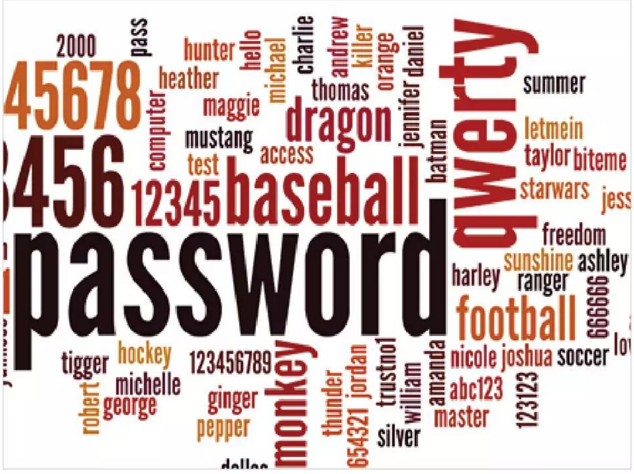
VISIBLE PASSWORD

Never write your password down on a Post-It note or somewhere near your computer. It's not too difficult for someone to visit your computer whilst you're on a coffee break and read the note.

PASSWORD :
ABC 123

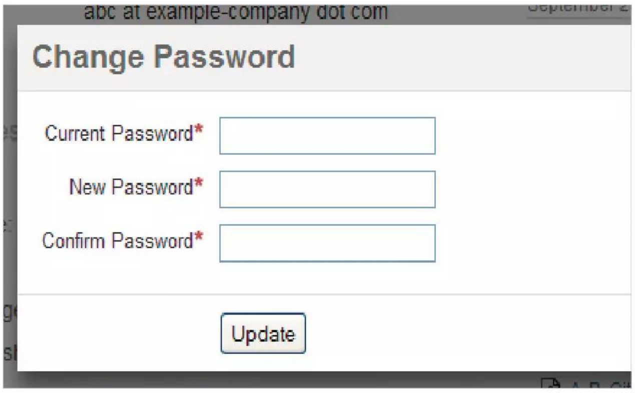
COMMON PASSWORDS

Try and avoid using common words in your password. Most password attacks are brute force, using dictionary words to gain access. Avoid using sequences of numbers, such as 1234. Instead, try inserting numbers, capital letters and symbols into words, such as C0m"o% instead of the word common, for example. However, avoid common words altogether if possible.


password
qwerty
baseball
dragon
football
monkey
12345
45678
2000
pass
hunter
hello
charlie
andrew
killer
heather
michael
thomas
orange
jennifer
daniel
maggie
computer
mustang
test
access
batman
summer
letmein
taylor
biteme
starwars
freedom
sunshine
ashley
harley
ranger
666666
tigger
hockey
123456789
michelle
robert
george
ginger
pepper
thunder
jordan
654321
trustno1
william
amanda
silver
nicole
joshua
soccer
abc123
master
123123

CHANGE REGULARLY

Regularly change your password. Most companies and good sites will require you to enter a new password that hasn't been used previously in the last few months every thirty days or so. If not, then you should actively keep changing your password yourself.


abc at example-company dot com

Change Password

Current Password*

New Password*

Confirm Password*

UNTRUSTED DEVICES

Never enter your password on a device or computer you don't trust. Entering your account details on a public computer, such as a kiosk or library, is dangerous as you don't know what protection these machines have nor whether they've already been compromised.

PUBLIC WI-FI

Try to avoid logging into certain sites when you're using public Wi-Fi. We've already covered how data on a public, free Wi-Fi access point can be intercepted. Your passwords, therefore, can be intercepted and viewed in plain text by a hacker.

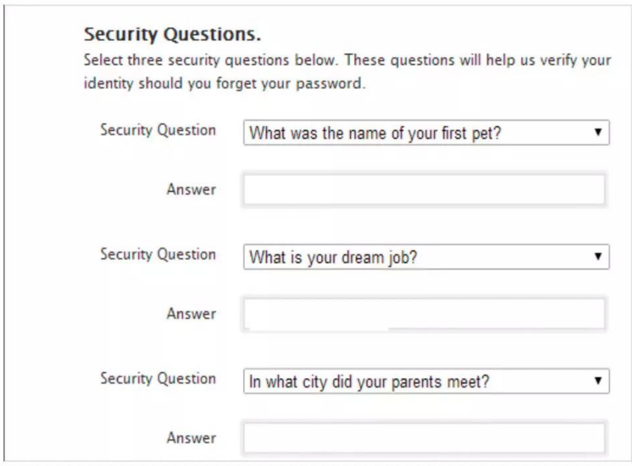
Free
Wi Fi
spot

LENGTHY PASSWORDS

Don't use short passwords. The longer they are, generally, the harder and more complex it will be should anyone try to crack it. A longer password that also utilises upper and lower case, numbers and symbols can't easily be viewed by any shoulder surfers.

SECURITY QUESTIONS

In addition to creating a password, some sites also offer a rescue security question. Sadly most of these questions are a little too easy to get the answers for. Questions such as Mother's Maiden name, first pet, town where you grew up, etc. can again be obtained by the clever hacker.


Security Questions.

Select three security questions below. These questions will help us verify your identity should you forget your password.

Security Question: What was the name of your first pet?

Answer

Security Question: What is your dream job?

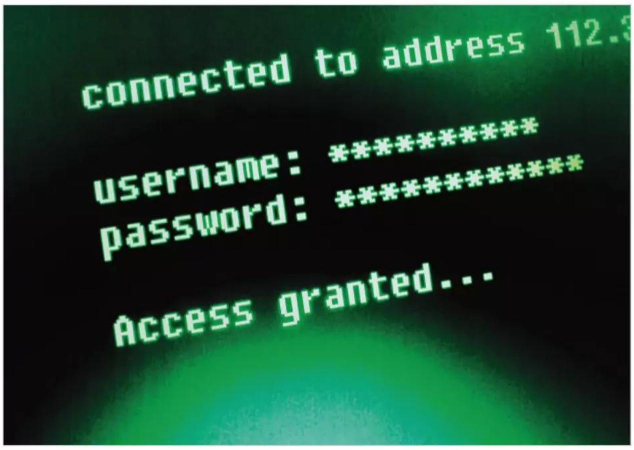
Answer

Security Question: In what city did your parents meet?

Answer

STRONG PASSWORDS

A strong password isn't going to be easy to remember at first. For example, something like 8%&KY4&$XzwMhfrk will take a hacker around a hundred thousand years to crack but it hardly flows off the tongue. Find a happy medium and make your password as strong as possible.



Password Generators and Tools

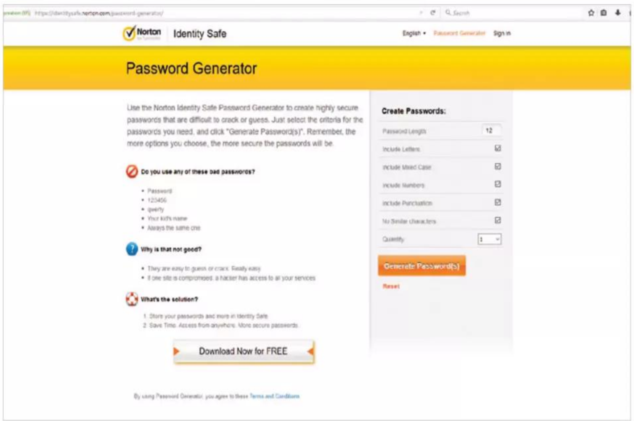
We've looked at some tips on what not to include when coming up with a strong password. However, it's not always as straight forward as that. Whilst some can come up with an elaborate and incredibly strong password, others struggle. Thankfully, there's help on offer.

Top Ten Password Generators

We live in an age where you don't have to sit with a dictionary and cryptic decoder to come up with an excellent password. There are many generators freely available to help you out. Here's our top ten.

NORTON IDENTITY SAFE PASSWORD GENERATOR

Norton by Symantec, offers a handy free password online generator. You can set the password length, include letters, mixed case, numbers, punctuation and no identical characters. You can find it at: **https://identitysafe.norton.com/password-generator/**.



Password Generator

Use the Norton Identity Safe Password Generator to create highly secure passwords that are difficult to crack or guess. Just select the criteria for the passwords you need, and click "Generate Password(s)". Remember, the more options you choose, the more secure the passwords will be.

Do you use any of these bad passwords?

- Password
- 123456
- qwerty
- Your kid's name
- Always the same one

Why is that not good?

- They are easy to guess or crack. Really easy
- If one site is compromised, a hacker has access to all your services

What's the solution?

1. Store your passwords and more in Identity Safe
2. Save Time. Access from anywhere. More secure passwords.

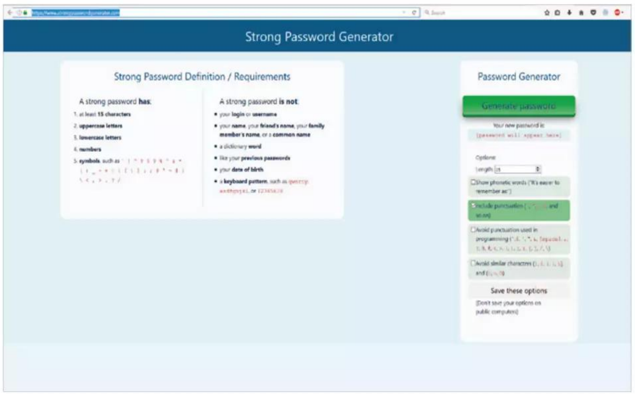
Create Passwords:

Password Length 12
Include Letters ☑
Include Mixed Case ☑
Include Numbers ☑
Include Punctuation ☑
No Similar characters ☑
Quantity 1

By using Password Generator, you agree to these Terms and Conditions

STRONG PASSWORD GENERATOR

Another great online resource that will create an incredibly strong password based on the options you choose. You can choose the length, punctuation and avoid similar characters but also display phonetic words to make it easier to remember. Try it out at: **https://strongpasswordgenerator.com/**.



Strong Password Definition / Requirements

A strong password **has**:

1. at least **15 characters**
2. **uppercase letters**
3. **lowercase letters**
4. **numbers**
5. **symbols**, such as

A strong password **is not**:

- your **login** or **username**
- your **name**, your **friend's name**, your **family member's name**, or a **common name**
- a dictionary **word**
- like your **previous passwords**
- your **date of birth**
- a **keyboard pattern**, such as qwerty, asdfghjkl, or 12345678

Password Generator

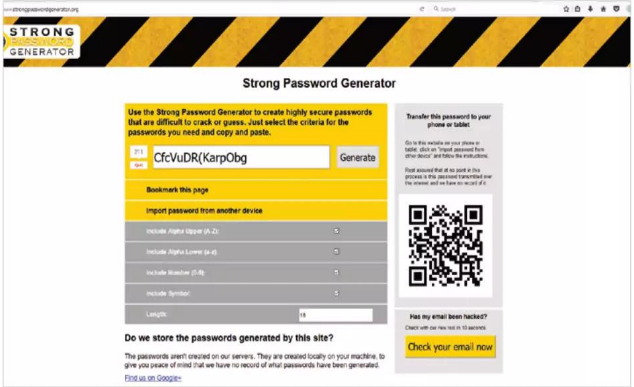
Your new password is:
[password will appear here]

Options
Length 15
☐ Show phonetic words ("It's easier to remember as")
☑ Include punctuation
☐ Avoid punctuation used in programming
☐ Avoid similar characters

(Don't save your options on public computers)

WIGHT HAT PASSWORD GENERATOR

This online password generator has been around for quite some time and has proved to be one of the best available for those after a unique and unbreakable password. There are ample options, and none of the passwords generated are stored remotely. Visit: **http://strongpasswordgenerator.org/** for more information.



Strong Password Generator

Use the Strong Password Generator to create highly secure passwords that are difficult to crack or guess. Just select the criteria for the passwords you need and copy and paste.

CfcVuDR(KarpObg

Include Alpha Upper (A-Z): ☑
Include Alpha Lower (a-z): ☑
Include Number (0-9): ☑
Include Symbol: ☑
Length: 15

Do we store the passwords generated by this site?

The passwords aren't created on our servers. They are created locally on your machine, to give you peace of mind that we have no record of what passwords have been generated.

Find us on Google+

Transfer this password to your phone or tablet

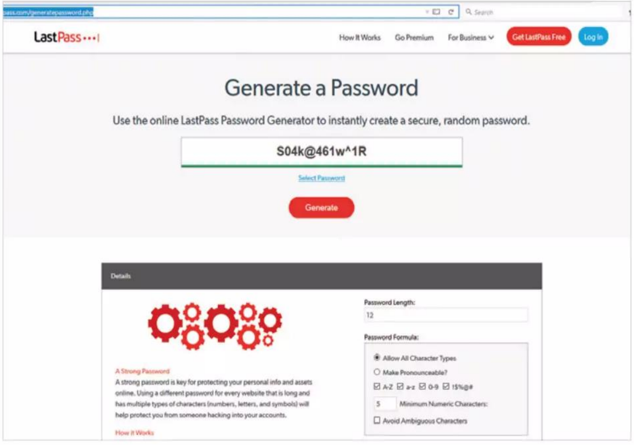
Go to this website on your phone or tablet, click on "Import password from other device" and follow the instructions.

Rest assured that at no point in this process is this password transmitted over the internet and we have no record of it.

Has my email been hacked?
Check with our new tool in 10 seconds

LASTPASS

LastPass is a popular password management program, which we'll look at in the next section; it also offers a free password generator. Found at **https://lastpass.com/generatepassword.php**, this excellent tool will help you create a strong and virtually unbreakable password in seconds.



Generate a Password

Use the online LastPass Password Generator to instantly create a secure, random password.

S04k@461w^1R

A Strong Password

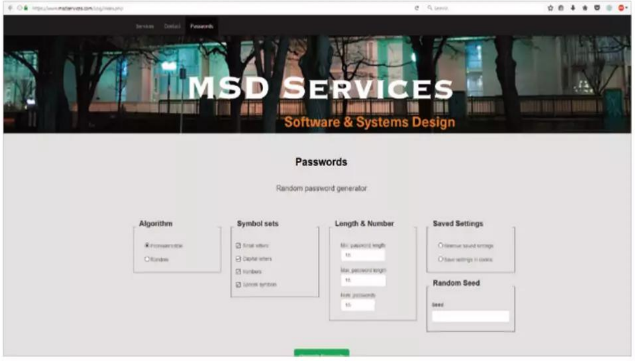
A strong password is key for protecting your personal info and assets online. Using a different password for every website that is long and has multiple types of characters (numbers, letters, and symbols) will help protect you from someone hacking into your accounts.

Password Length:
12

Password Formula:
● Allow All Character Types
○ Make Pronounceable?
☑ A-Z ☑ a-z ☑ 0-9 ☑ !$%@#
5 Minimum Numeric Characters:
☐ Avoid Ambiguous Characters

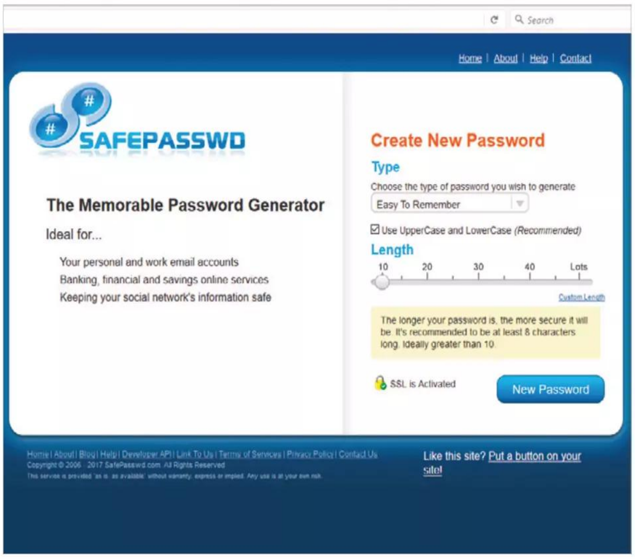
MSD SERVICES

An interesting site this, one that will allow you to create multiple unique passwords, based on length, upper and lower case, number and symbols as well as whether the end result will be pronounceable or completely random. It's at **https://msdservices.com/apg/index.php** for those after several passwords.


MSD SERVICES
Software & Systems Design
Passwords
Random password generator
Algorithm
Symbol sets
Length & Number
Saved Settings
Random Seed

SAFEPASSWD

Another great site to have in your password arsenal. SafePasswd has been around since 2006 and is regarded as one of the best online password generators. The options are many and with them you can create something truly impossible to crack. You can find it at: **https://www.safepasswd.com/**.


Search
Home | About | Help | Contact
SAFEPASSWD
Create New Password
Type
Length
10
20
30
40
Lots
Custom Length
New Password
Home | About | Blog | Help | Developer API | Link To Us | Terms of Services | Privacy Policy | Contact Us

The Memorable Password Generator

Ideal for...

Your personal and work email accounts
Banking, financial and savings online services
Keeping your social network's information safe

Choose the type of password you wish to generate

Easy To Remember

☑ Use UpperCase and LowerCase *(Recommended)*

The longer your password is, the more secure it will be. It's recommended to be at least 8 characters long. Ideally greater than 10.

SSL is Activated

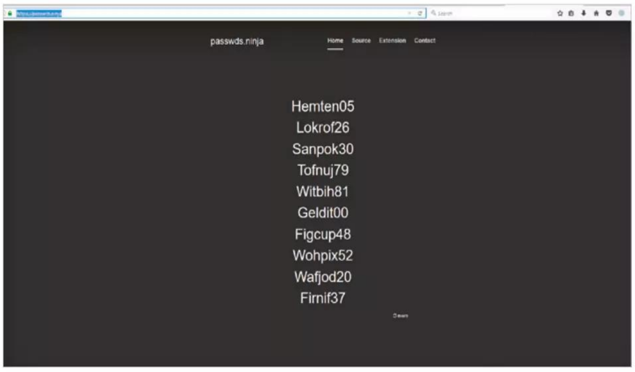
Copyright © 2006 - 2017 SafePasswd.com. All Rights Reserved

This service is provided "as is", "as available" without warranty, express or implied. Any use is at your own risk.

Like this site? Put a button on your site!

PASSEDS.NINJA

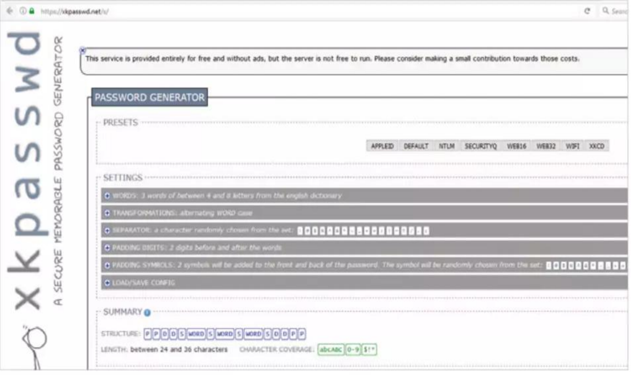
This is a quick and easy online password generator. You won't get any options or added extras, you simply click a button and ten unique passwords will be displayed for you to choose from. It's worth looking into for a quick solution to password creation; **https://passwds.ninja/**.


passwds.ninja
Home
Source
Extension
Contact

Hemten05
Lokrof26
Sanpok30
Tofnuj79
Witbih81
Geldit00
Figcup48
Wohpix52
Wafjod20
Firnif37

XKPASSWRD

This site is powered by the XKPasswd.pm Perl module, which offers a range of settings to help create a unique and very strong password. There are plenty of options to choose from and you can save and load your preferred configuration for later. It's at: **https://xkpasswd.net/s/** if you want to check it out.


xkpasswd
A SECURE MEMORABLE PASSWORD GENERATOR
PASSWORD GENERATOR
PRESETS
APPLEID
DEFAULT
NTLM
SECURITYQ
WEB16
WEB32
WIFI
XKCD
SETTINGS
LOAD/SAVE CONFIG
SUMMARY

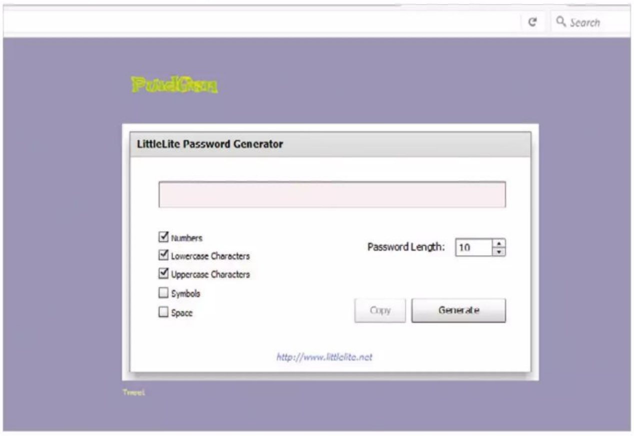
This service is provided entirely for free and without ads, but the server is not free to run. Please consider making a small contribution towards those costs.

WORDS: 3 words of between 4 and 8 letters from the english dictionary
TRANSFORMATIONS: alternating WORD case
SEPARATOR: a character randomly chosen from the set:
PADDING DIGITS: 2 digits before and after the words
PADDING SYMBOLS: 2 symbols will be added to the front and back of the password. The symbol will be randomly chosen from the set:

STRUCTURE: P P D D S WORD S WORD S WORD S D D P P
LENGTH: between 24 and 26 characters CHARACTER COVERAGE: abcABC 0-9 $!*

LITTLELITE PASSWORD GENERATOR

Another simple but easy to use and good online password generator. LittleLite offers some options, including password length, number, upper and lower case, symbols and spaces. It's found at **http://www.littlelite.net/pwdgen/** and certainly worth considering bookmarking.

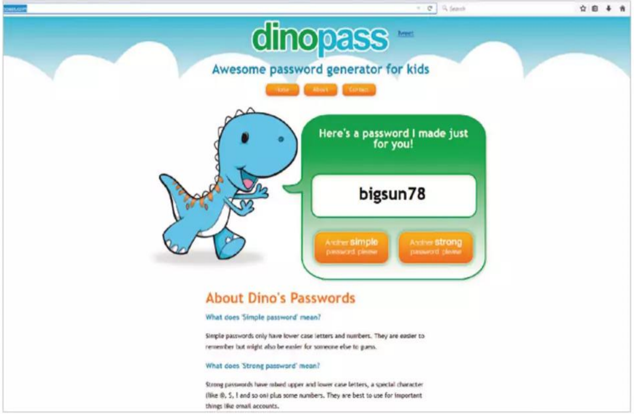

Search
PwdGen
LittleLite Password Generator
Copy
Generate
http://www.littlelite.net

☑ Numbers
☑ Lowercase Characters
☑ Uppercase Characters
☐ Symbols
☐ Space

Password Length: 10

DINOPASS

For kids at school or when online, DinoPass is an excellent resource that will help them come up with a memorable, yet strong password. You can choose between a simple or strong password type, depending on where it's going to be used and there's meanings of each to help out, too. You can find it at: **http://www.dinopass.com/**.


dinopass
Awesome password generator for kids
Here's a password I made just for you!
Another simple password please
Another strong password please
About Dino's Passwords

bigsun78

What does 'Simple password' mean?

Simple passwords only have lower case letters and numbers. They are easier to remember but might also be easier for someone else to guess.

What does 'Strong password' mean?

Strong passwords have mixed upper and lower case letters, a special character (like @, $, ! and so on) plus some numbers. They are best to use for important things like email accounts.

Top Ten Password Managers

Creating uncrackable passwords is one thing, remembering them for each of the services that require one is something else entirely. The reason why most people opt for a single password for all their accounts is simply due to not being able to remember them all. This is where password managers help.

Manage Those Passwords

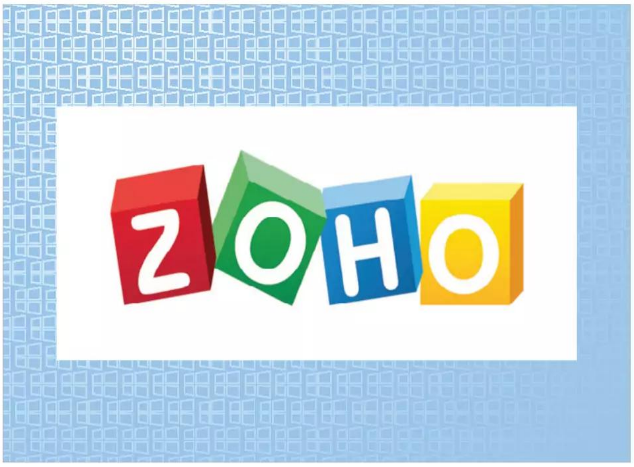
Password managers differ in what they offer, how they work and what optional extras they provide. Therefore it can be tricky to find one that fits the bill. Some are free, others cost a monthly or annual fee; here are ten to consider.

LASTPASS

LastPass, which also offer a free password generator, is regarded as one of the finest managers available. There's a free version that offers unlimited password storage, cross-platform access, two-factor authentication and elevated levels of encryption. There's also a Premium version that offers a lot more, including 1GB of encrypted file storage and higher levels of encryption.

ZOHO VAULT

Zoho Vault is another excellent password management application. With a free version on offer, moving up to Enterprise levels for just €7 per month, Zoho allows unlimited passwords, access from all platforms, password tracking, offline access, auto-login for websites and much more.



STICKY PASSWORD

Sticky Password is available both as free or Premium versions, costing just £24 and offers two-factor authentication, autofill for websites, advanced biometrics; it's also available on all major platforms. The Premium version goes further with cloud backup and syncing and with every license purchased a Manatee is saved. Certainly worth considering.

StickyPassword
securing your personal data

DASHLANE

With free, Premium and Business options available, Dashlane covers a huge user base. Its features are many and it offers the user a high degree of encryption and security alongside all the usual auto-filling, two-factor authentication and the ability to export data.

KEEPER

Keeper is a powerful and feature rich password manager that has Individual, Family and Business plans available for £20.99, £44.99, and £22 per year respectively. With unlimited password storage, unlimited device syncing, finger print login and secure cloud backup, amongst others, it's certainly one to consider.

KEEPASS

KeePass is a freely available, open source password manager that's regularly updated and comes with a long list of interesting features. You can import and export password data, it's fully portable so there's no installation required and it adheres to 256-bit AES encryption.

1PASSWORD

1Password offer an individual and Family plan for as little as £2.30 and £4 per year. With it you can access password across all your devices and operating systems; there's offline access, automatic synching, 1GB of secure storage available and a 365 day password history recovery.

PASSWORD BOSS

Password Boss offers both free and Premium plans, with the Premium plan costing around £24 per year. There are ample features to enjoy, including cross platform support, full military encryption, cloud synching and more.

PASSWORD
BOSS

TRUE KEY

True Key is an excellent password manager with a free and Premium plan available; the Premium plan costing around £29.99 a year. It's unique in that it utilises facial recognition as well as finger print, and integration with Windows Hello. There are plenty of other options available too, so it's worth looking into.

LOGMEONCE

LogMeOnce is an award-winning password manager that incorporates many interesting features. It's ultimate selling point, however, is a passwordless operation, whereby you are able to log in to any website or service just by using facial recognition. Prices do vary across the Premium, Professional and Ultimate editions but the personal version is free.

Logme Once
Password Security with Convenience

Shopping Online and Security

Windows 10 is continually improving and as such the new updates have brought a more customisable degree of control over the operating system's privacy configuration; something that Microsoft has always been criticised for in the past.

The length of breadth of online shopping is far too vast to cover every conceivable angle here. So rather than focus on particular elements, here are ten online shopping security tips to apply across the board.

> “10 Online Shopping Security Tips”

RUSH BUYING Don't be fooled into rush buying something that's at a ridiculously low price. If a site is selling an iPhone for £20, then it's more than likely to be a ruse to lure you in and steal your money.

FAKE SITES Ensure that you're buying from a real website. Fake sites are remarkably easy to create by the clever hacker and are designed to steal your transactions. Be wary of sites other than the big names. While smaller online shops are fine, just look into the type of security it's using and do some research before purchasing.

BOGUS EMAIL Strange email addresses are something to look out for with suspect online shops. If the support email or contact information for the site is something like: ebayhelp@gmail.com instead of support@ebay.com, then there's most definitely something wrong.

USE HTTPS

Remember to load up the online shop using HTTPS instead of HTTP. This will ensure that the transactions and data sent between you and it are encrypted to the highest possible levels. If possible, use a browser add-on such as HTTPS Everywhere.

AVOID PUBLIC Wi-Fi

Tempting as it may be, don't use a public Wi-Fi access point to conduct any online shopping. For one, you could be attached to an Evil Twin Wi-Fi point, where the hacker is filtering all information through their system and two, all your data can be intercepted and potentially read.

3RD PARTY SECURITY

Invest in one of the many third-party antivirus and malware suites, such as Bitdefender. These programs also offer extra security when shopping online and can help prevent any hacking or data interception from happening whilst the transactions are in progress. They can also check the site you're buying from, too.

BANK TRANSACTIONS

Always keep an eye on your bank account and the transactions that go on after you've conducted online shopping. This will help you get an idea of what's going on and should something suddenly crop up that looks suspicious, then you're able to inform your bank before too much damage is done.

STRONG PASSWORDS

Use a strong and unique password for all your shopping sites. Occasionally, although not often, websites can be hacked and the database of users is leaked. If your password is strong enough, it will stand up to any decryption methods.

SHOPPING APPS

If possible, always use an online shop's dedicated app rather than the standard website. Websites can be compromised, however apps from iTunes and the Windows Store, for example, can't be altered by a third-party.

PAYPAL

If possible use PayPal or a Credit Card as opposed to a Debit Card. Credit cards have an extra layer of protection and legal standing than that of a debit card; PayPal features many protection elements within its accounts too.

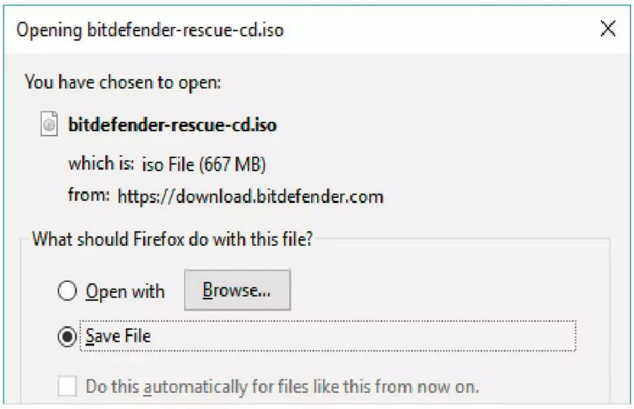
How to Remove a Virus or Malware from a Windows PC

So far we've looked at ways to prevent getting scammed or indeed getting malware on your system but what if you're unlucky enough to already have some form of digital infection? Thankfully, there's a way to remove malware and viruses from your computer.

Malware Busters

For this tutorial let's use a preconfigured rescue disk from Bitdefender. You need to transfer, or burn, the disk contents to a CD or a USB stick and boot into the safe environment through one of those mediums.

STEP 1 Make sure you have a blank CD or a USB stick that's at least 1GB in size. The Bitdefender Rescue Disk is downloaded as an ISO (which is an image file containing all the disk information) and can be downloaded from www.download.bitdefender.com/rescue_cd/latest/bitdefender-rescue-cd.iso.


Opening bitdefender-rescue-cd.iso

You have chosen to open:

bitdefender-rescue-cd.iso

which is: iso File (667 MB)

from: https://download.bitdefender.com

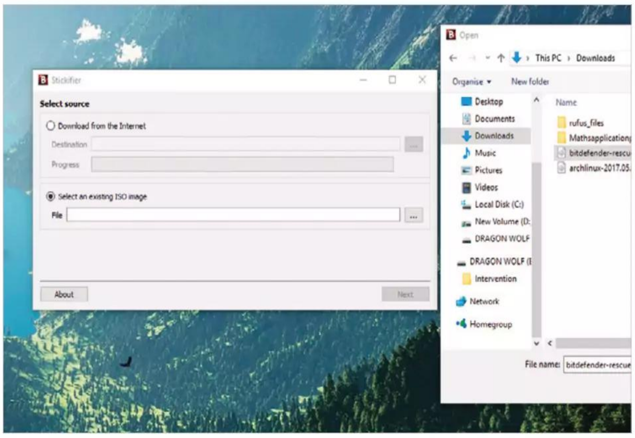
What should Firefox do with this file?

○ Open with [Browse...]

● Save File

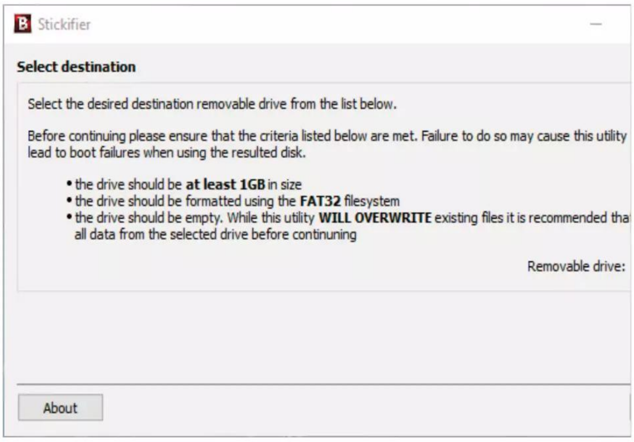
☐ Do this automatically for files like this from now on.

STEP 2 To transfer the ISO to USB download Stickifier, which is an executable that doesn't require any installation. Insert your USB stick and double-click Stickifier. Click the Select an Existing ISO Image option followed by the three full-stops and using Windows Explorer, locate the downloaded Bitdefender Rescue ISO. Click the Open button to select the image and continue with the process.


Stickifier
Select source
○ Download from the Internet
Destination
Progress
● Select an existing ISO image
File
...
About
Next
Open
This PC › Downloads
Organise ▾
New folder
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
New Volume (D:
DRAGON WOLF
DRAGON WOLF (
Intervention
Network
Homegroup
Name
rufus_files
Mathsapplication
bitdefender-rescu
archlinux-2017.05.
File name:

File name: bitdefender-rescue

STEP 3 Click the Next button and using the drop-down menu next to Removeable Drive choose the drive letter of your USB stick. Click Next to start the transfer of the image. Once the image is transferred click the Finish button and remove the USB stick and power off your computer.


Stickifier

Select destination

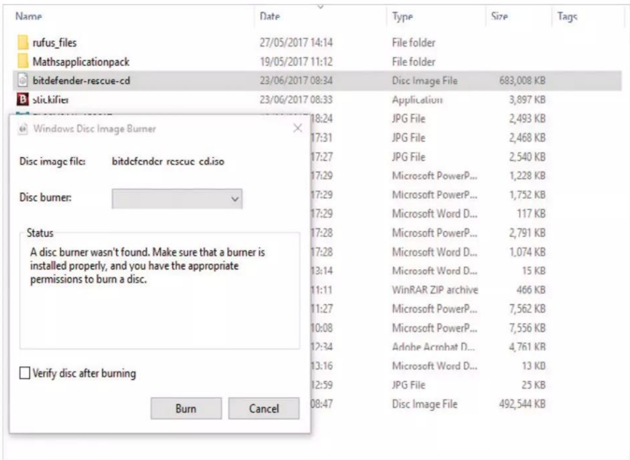
Select the desired destination removable drive from the list below.

Before continuing please ensure that the criteria listed below are met. Failure to do so may cause this utility lead to boot failures when using the resulted disk.

- the drive should be **at least 1GB** in size
- the drive should be formatted using the **FAT32** filesystem
- the drive should be empty. While this utility **WILL OVERWRITE** existing files it is recommended tha all data from the selected drive before continuning

Removable drive:

STEP 4 If you're using a CD, start by inserting the CD into the drive. Locate the downloaded Bitdefender Rescue ISO, right-click it and choose Burn Disc Image from the context menu. Tick the Verify disc after burning option and click the Burn button to start the process. Once the ISO is burnt to the disc, you can power off your computer.


Name	Date	Type	Size	Tags
rufus_files	27/05/2017 14:14	File folder		
Mathsapplicationpack	19/05/2017 11:12	File folder		
bitdefender-rescue-cd	23/06/2017 08:34	Disc Image File	683,008 KB	
stickifier	23/06/2017 08:33	Application	3,897 KB	
	18:24	JPG File	2,493 KB	
	17:31	JPG File	2,468 KB	
	17:27	JPG File	2,540 KB	
	17:29	Microsoft PowerP...	1,228 KB	
	17:29	Microsoft PowerP...	1,752 KB	
	17:29	Microsoft Word D...	117 KB	
	17:28	Microsoft PowerP...	2,791 KB	
	17:28	Microsoft Word D...	1,074 KB	
	13:14	Microsoft Word D...	15 KB	
	11:11	WinRAR ZIP archive	466 KB	
	11:27	Microsoft PowerP...	7,562 KB	
	10:08	Microsoft PowerP...	7,556 KB	
	12:34	Adobe Acrobat D...	4,761 KB	
	13:16	Microsoft Word D...	13 KB	
	12:59	JPG File	25 KB	
	08:47	Disc Image File	492,544 KB	

Windows Disc Image Burner

Disc image file: bitdefender-rescue-cd.iso

Disc burner:

Status

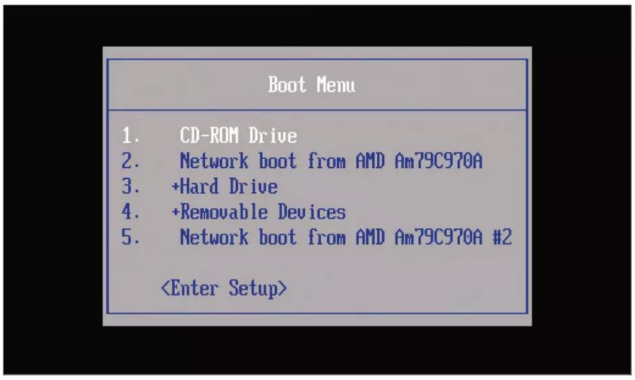
A disc burner wasn't found. Make sure that a burner is installed properly, and you have the appropriate permissions to burn a disc.

☐ Verify disc after burning

Burn
Cancel

STEP 5

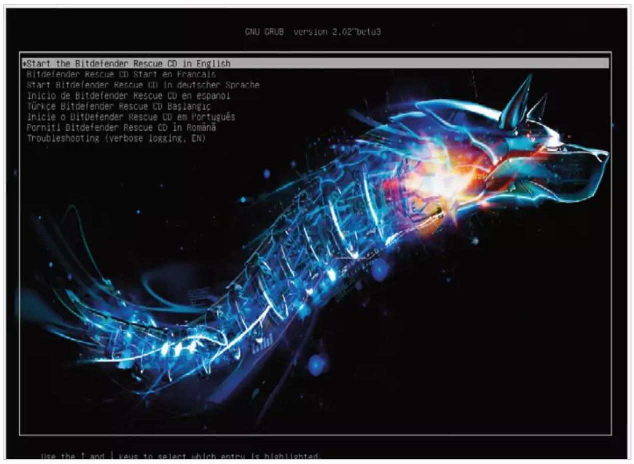
You now need to allow your PC to boot up into the Bitdefender Rescue CD environment. Power up your PC and open the Boot Option Menu. This could be accessed by pressing F12, depending on the make and manufacturer of your PC motherboard. With the boot options available, select either the CD or USB stick and press Enter.



```
Boot Menu

1.  CD-ROM Drive
2.  Network boot from AMD Am79C970A
3. +Hard Drive
4. +Removable Devices
5.  Network boot from AMD Am79C970A #2

   <Enter Setup>
```

STEP 6

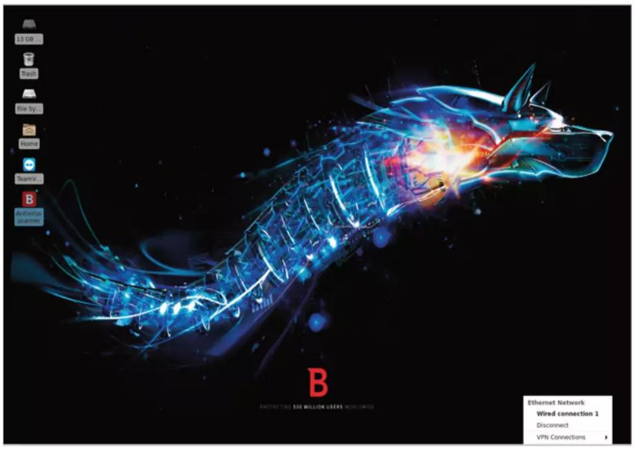
The PC will now boot into the Bitdefender Rescue Disc environment. This is a custom Linux operating system with all the necessary Bitdefender security tools preinstalled. First, you need to choose which language to load the environment. Use the arrow keys, and press Enter for your language choice.



```
GNU GRUB  version 2.02~beta3

*Start the Bitdefender Rescue CD in English
 Bitdefender Rescue CD Start en Francais
 Start Bitdefender Rescue CD in deutscher Sprache
 Inicio de Bitdefender Rescue CD en espanol
 Türkçe Bitdefender Rescue CD Başlangıç
 Inicie o BitDefender Rescue CD em Português
 Porniti Bitdefender Rescue CD în Română
 Troubleshooting (verbose logging, EN)
```

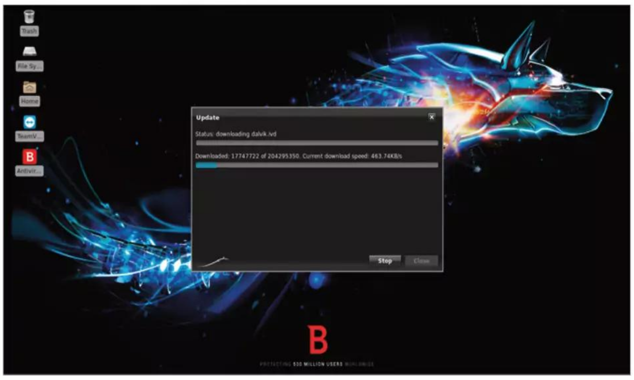
STEP 7

Ideally you should use a wired Internet connection but if you're on wireless, click on the network icon in the bottom right of the desktop to establish a connection with your router. Once you're connected to the Internet, double-click the red Bitdefender icon on the desktop, labelled Antivirus Scanner.



STEP 8

You need to accept the license agreement notification first. Tick the I agree box, followed by clicking the Continue button. The virus scanning software will then start to automatically update itself with the latest virus definitions from the Bitdefender servers. The process won't take too long, so let it run through the update.



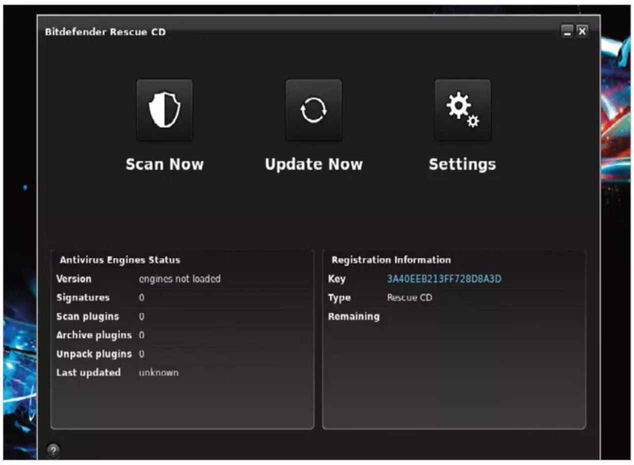
Update

Status: downloading dalvik.ivd

Downloaded: 17747722 of 204295350. Current download speed: 463.74KB/s

STEP 9

Once the update is complete you're taken to the main Bitdefender Rescue CD antivirus interface. The three main options: Scan Now, Update Now and Settings are fairly self-explanatory; the Settings allows you to set a few more options regarding the scan, however the defaults will suffice.



Antivirus Engines Status

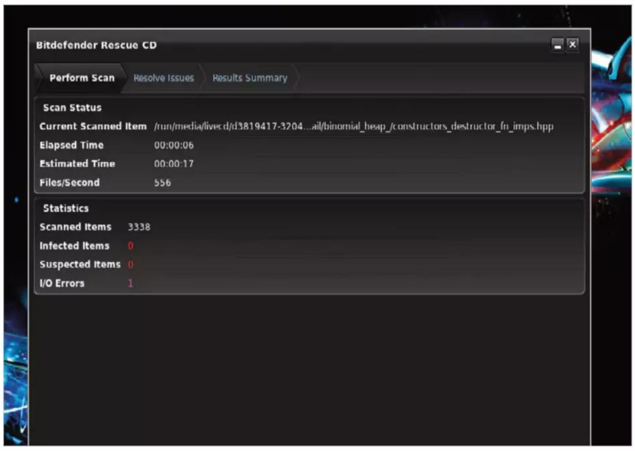
Version engines not loaded
Signatures 0
Scan plugins 0
Archive plugins 0
Unpack plugins 0
Last updated unknown

Registration Information

Key 3A40EEB213FF728D8A3D
Type Rescue CD
Remaining

STEP 10

To remove a virus on your PC, click on the Scan Now button. Select the drive you wish to scan and click the Open button to commence scanning the system. Any viruses found will be detailed along with options for removal. The process may take some time, so be prepared for a lengthy wait.



Scan Status

Current Scanned Item /run/media/livecd/d3819417-3204...ail/binomial_heap_/constructors_destructor_fn_imps.hpp
Elapsed Time 00:00:06
Estimated Time 00:00:17
Files/Second 556

Statistics

Scanned Items 3338
Infected Items 0
Suspected Items 0
I/O Errors 1

Advanced Security Tips

If you want to improve your Windows security further, then this section looks at more advanced ways and means in which you can achieve that goal. We cover firewalls, sandboxing and virtual environments and how to tell which programs are communicating beyond your home network.

Our easy to follow tutorials will help you create a reliable backup of Windows 10 and all your data, so should something happen you'll be able to restore your files with confidence.

96 Windows 10 Privacy Settings
98 How to Check which Apps are Sending Information
100 What is a firewall?
102 Improving the Windows 10 Firewall
104 Creating a Security Plan
106 Windows Security Checklist
108 What is a Sandbox?
110 Running Windows 10 as a Sandbox
112 Installing VirtualBox
114 Installing Windows 10 in VirtualBox
116 Creating VirtualBox Snapshots of Windows 10
118 Create a Windows 10 Recovery Drive
120 How to Back Up Windows 10
122 How to Create a Windows 10 System Image
124 Extreme Windows 10 Lockdown Tips
126 Cyber and Windows Quiz
128 What the Experts Say

Windows 10 Privacy Settings

Windows 10's new updates and special edition updates have brought a more customisable degree of control over the operating system's privacy configuration; something that Microsoft has always been criticised for in the past.

Going Private

Windows 10 is said to be the last true Windows desktop release, with the Redmond company now opting for a rolling release cycle, that will add or remove features over time through regular updates.

There are many advantages to this particular setup. A Windows 10 user will always be up to date with regards to security, options and support. Any new hardware that's released will be added to the vast driver database that Windows 10 already uses and it will operate at its maximum potential. Microsoft can gradually roll out features that would require a brand new operating system, thus maximising the capabilities of the OS. Of course, the company can charge for certain additional features that would ordinarily be a part of the OS, such as a media centre for example.

However, profit margins aside, it's the rolling security and updates that the user will benefit greatly from. As Microsoft evolves Windows 10, user and developer feedback can help improve the way the OS protects its user base. A prime example is the new privacy settings available post-Fall Creators Update, which was gradually rolled out to Windows 10 PCs around late October 2017. The privacy settings and options that are now on offer are a radical improvement over the previous, rather bleak, features that came with the original Windows 10 setup. Now, the user has greater control over what the OS can and cannot do to affect an individual's privacy.

Providing you've applied the Fall Creators Update, you can view the current privacy options by clicking the Windows Start button and typing privacy into the search box. Click on the Privacy Settings option, with a padlock icon, and the core privacy options window will open. There are, at the time of writing, nineteen different options available to browse through. Each option, when clicked, will display a subset of available options that can then be enabled or disabled and turned on or off, depending on your preference.

For example the first option, General, offers the user a choice of opting for advertising via apps, allowing websites to provide locally relevant content based on the user's language list and allowing Windows 10 to track how an app is launched to improve search results. Whilst that in itself doesn't sound too much like your privacy is being infiltrated, there are those who don't want the installed apps and the OS having too much knowledge of where they are and what to advertise. Like most privacy options, it's a personal preference as to what you're happy sharing with the system and its connected technologies. Whilst opting to turn every privacy setting on will inevitably open your use of Windows 10 up to whoever or whatever is readily receiving the information, likewise turning everything off will effectively hide you (to some degree); but at the cost of possible loss of available features. There's a fine balance needed to get the best from your privacy and still enjoying Windows 10's many features.

There are some interesting additions to the Fall Creators Update privacy settings, which are certainly worth looking over, if you want a best of both worlds approach to privacy and features.

Location – The Location option will allow Windows 10 and its apps to use your current location to specialise any content. It's innocent enough but for added privacy it's worth considering turning it off.

Camera – This is an excellent addition that will define which installed apps have access to the computer's webcam. You can turn off app access to the camera globally or browse through the apps to decide which has access, or not.

Microphone – The same applies for the computer's microphone; which apps can access it or not, and whether you want to globally turn it off.

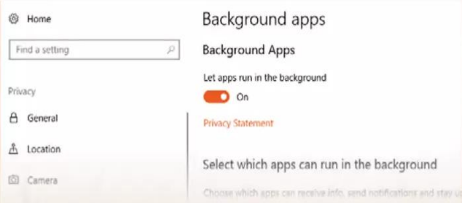
Contacts – The Contacts section details which apps can have access to your current Windows account contacts. Disabling this globally may have a severe impact on how some apps, such as Skype and email work.

Radios – This option will define which apps can control hardware such as the computer's Bluetooth device, Wi-Fi or any other kind of wireless receiver. Obviously, some apps will require access to share information or allow access to shared areas.

Background Apps – Windows 10's background task handling is far better than in previous versions of the operating system. Memory is released as apps drop into the background, as is processor allocation. However, you can further define which apps will be allowed to run in the background with this option.

Taking time to go through each of the available options is something every Windows 10 user should do. This way you become familiar with how the OS shares your account data and what exactly has access to your Windows 10 computer and its hardware.

Which apps are allowed to run silently in the background whilst you work? You can decide whether they do, or not.. . .



Background apps

Background Apps

Let apps run in the background

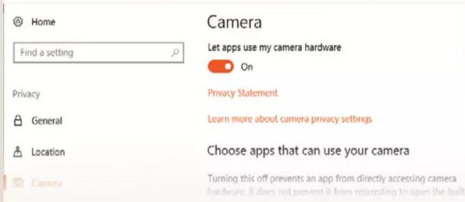
On

Privacy Statement

Select which apps can run in the background

Choose which apps can receive info, send notifications and stay u

You can control which apps have access to the computer's webcam. Handy for keeping track of your privacy. . .



Camera

Let apps use my camera hardware

On

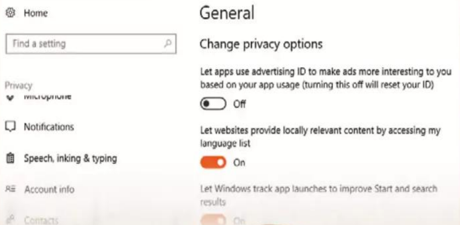
Privacy Statement

Learn more about camera privacy settings

Choose apps that can use your camera

Turning this off prevents an app from directly accessing camera

Click the Windows Start button and type privacy, click on the Privacy Settings link and you see this screen . . .



General

Change privacy options

Let apps use advertising ID to make ads more interesting to you based on your app usage (turning this off will reset your ID)

Off

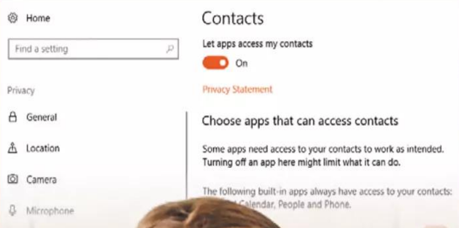
Let websites provide locally relevant content by accessing my language list

On

Let Windows track app launches to improve Start and search results

On

Windows 10's apps can access almost every element of your account, including your contacts. . .



Contacts

Let apps access my contacts

On

Privacy Statement

Choose apps that can access contacts

Some apps need access to your contacts to work as intended. Turning off an app here might limit what it can do.

The following built-in apps always have access to your contacts: Calendar, People and Phone.

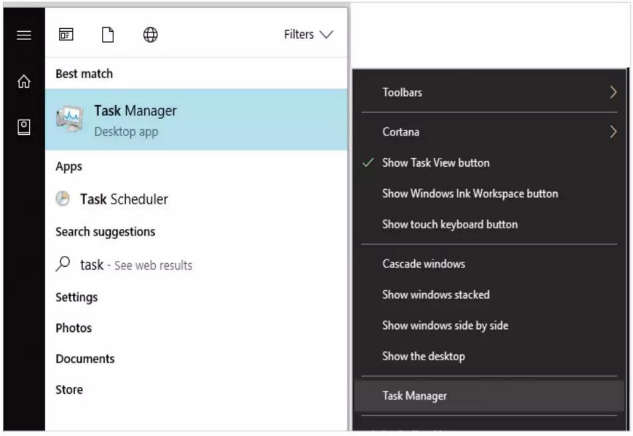
How to Check which Apps are Sending Information

Most Windows 10 apps and programs have some element of code that will attempt to communicate with an external source. That communication could be to check for the latest version, or patches and updates, or it could be malicious software sending personal data.

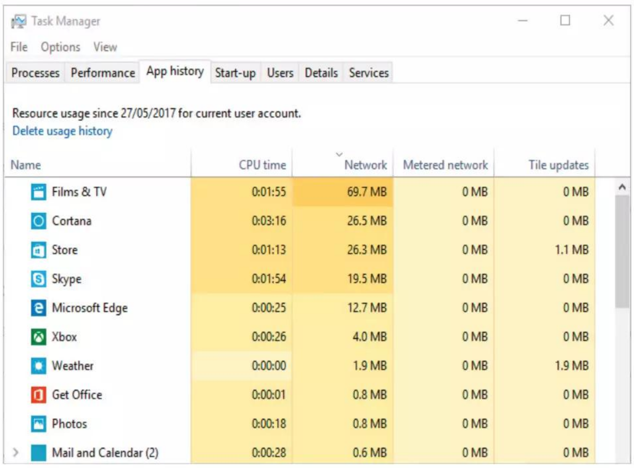
Look Who's Talking

There are a number of ways in which you're able to view which programs and apps are sending data to Internet and external sources. Some methods are better than others, so it's worth trying them all to see which works best for you.

STEP 1 The first port of call to help monitor what apps are accessing the Internet is Task Manager. Click the Windows Start button and type task, then click the Task Manager result in the search box. You can also right-click the taskbar and select Task Manager from the available option in the menu.


Filters
Best match
Task Manager
Desktop app
Apps
Task Scheduler
Search suggestions
task - See web results
Settings
Photos
Documents
Store
Toolbars
Cortana
Show Task View button
Show Windows Ink Workspace button
Show touch keyboard button
Cascade windows
Show windows stacked
Show windows side by side
Show the desktop
Task Manager

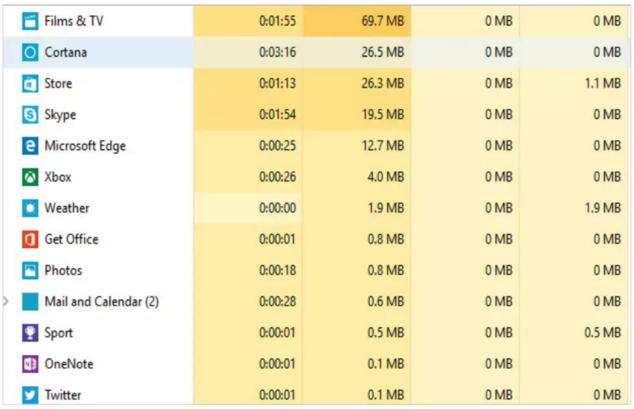
STEP 2 With Task Manager displayed, click the More Details arrow (if it's available). This will expand the Task Manager options. From here, click the App History tab and then the Network column so that there's a downward pointing arrow above it. This indicates network use in a descending order of amount of data sent.


Task Manager
File Options View
Processes Performance App history Start-up Users Details Services

Resource usage since 27/05/2017 for current user account.
Delete usage history

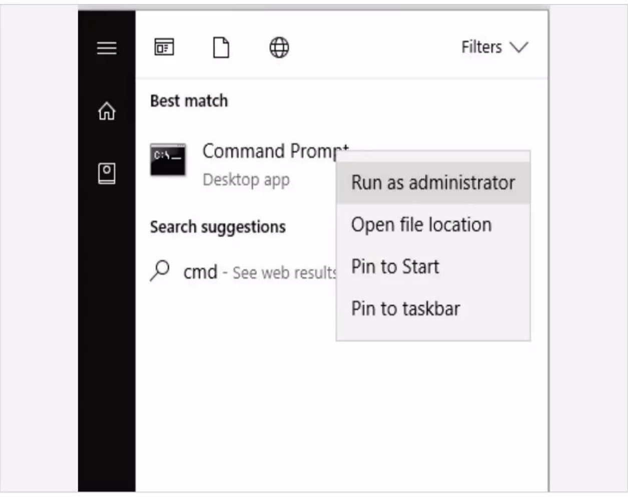
Name	CPU time	Network	Metered network	Tile updates
Films & TV	0:01:55	69.7 MB	0 MB	0 MB
Cortana	0:03:16	26.5 MB	0 MB	0 MB
Store	0:01:13	26.3 MB	0 MB	1.1 MB
Skype	0:01:54	19.5 MB	0 MB	0 MB
Microsoft Edge	0:00:25	12.7 MB	0 MB	0 MB
Xbox	0:00:26	4.0 MB	0 MB	0 MB
Weather	0:00:00	1.9 MB	0 MB	1.9 MB
Get Office	0:00:01	0.8 MB	0 MB	0 MB
Photos	0:00:18	0.8 MB	0 MB	0 MB
Mail and Calendar (2)	0:00:28	0.6 MB	0 MB	0 MB

STEP 3 This is a reasonably accurate way of viewing which installed programs have been accessing the outside world. The amount of data being sent to and from your PC can be quite illuminating, and surprising, as you may never even realise you have a particular app installed never mind that it's communicating with an external source.

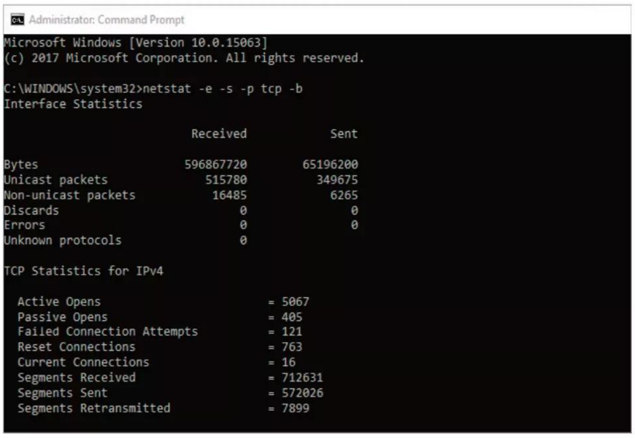


Films & TV	0:01:55	69.7 MB	0 MB	0 MB
Cortana	0:03:16	26.5 MB	0 MB	0 MB
Store	0:01:13	26.3 MB	0 MB	1.1 MB
Skype	0:01:54	19.5 MB	0 MB	0 MB
Microsoft Edge	0:00:25	12.7 MB	0 MB	0 MB
Xbox	0:00:26	4.0 MB	0 MB	0 MB
Weather	0:00:00	1.9 MB	0 MB	1.9 MB
Get Office	0:00:01	0.8 MB	0 MB	0 MB
Photos	0:00:18	0.8 MB	0 MB	0 MB
Mail and Calendar (2)	0:00:28	0.6 MB	0 MB	0 MB
Sport	0:00:01	0.5 MB	0 MB	0.5 MB
OneNote	0:00:01	0.1 MB	0 MB	0 MB
Twitter	0:00:01	0.1 MB	0 MB	0 MB

STEP 4 Another excellent method is by using the Netstat command. Click on the Windows Start button and enter **cmd**, then right-click the Command Prompt option and choose Run as Administrator from the menu. When the message to authenticate the action pops up, click on Yes.

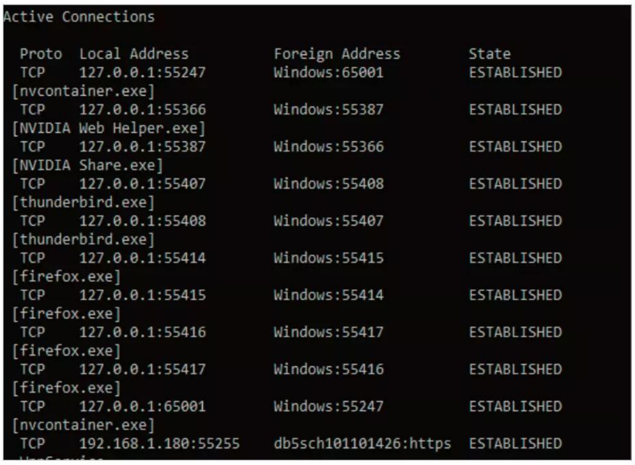

Filters
Best match
Command Prompt
Desktop app
Run as administrator
Open file location
Pin to Start
Pin to taskbar
Search suggestions
cmd - See web results

STEP 5 With the command prompt open enter the following: **netstat -e -s -p tcp -b**. The information populates the command prompt box quickly, so you need to scroll back up to the top to see it in its entirety.



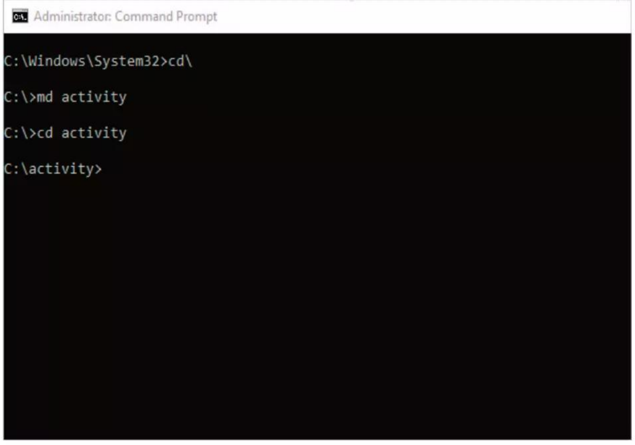
```
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>netstat -e -s -p tcp -b
Interface Statistics

                           Received            Sent

Bytes                     596867720        65196200
Unicast packets              515780          349675
Non-unicast packets           16485            6265
Discards                          0               0
Errors                            0               0
Unknown protocols                 0

TCP Statistics for IPv4

  Active Opens                        = 5067
  Passive Opens                       = 405
  Failed Connection Attempts          = 121
  Reset Connections                   = 763
  Current Connections                 = 16
  Segments Received                   = 712631
  Segments Sent                       = 572026
  Segments Retransmitted              = 7899
```

STEP 6 What you're looking at here is a list of programs, from the column to the far left, with the IP address of its source and the destination address in the middle column; with a third column detailing if the connection is established or not. It can be confusing to view at first but after a moment or two it should begin to make sense.



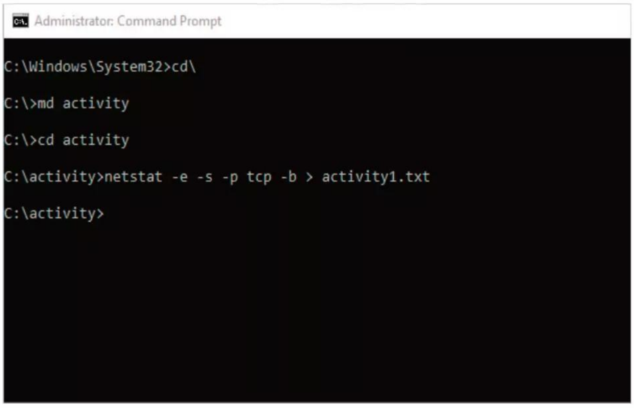
```
Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:55247        Windows:65001          ESTABLISHED
 [nvcontainer.exe]
  TCP    127.0.0.1:55366        Windows:55387          ESTABLISHED
 [NVIDIA Web Helper.exe]
  TCP    127.0.0.1:55387        Windows:55366          ESTABLISHED
 [NVIDIA Share.exe]
  TCP    127.0.0.1:55407        Windows:55408          ESTABLISHED
 [thunderbird.exe]
  TCP    127.0.0.1:55408        Windows:55407          ESTABLISHED
 [thunderbird.exe]
  TCP    127.0.0.1:55414        Windows:55415          ESTABLISHED
 [firefox.exe]
  TCP    127.0.0.1:55415        Windows:55414          ESTABLISHED
 [firefox.exe]
  TCP    127.0.0.1:55416        Windows:55417          ESTABLISHED
 [firefox.exe]
  TCP    127.0.0.1:55417        Windows:55416          ESTABLISHED
 [firefox.exe]
  TCP    127.0.0.1:65001        Windows:55247          ESTABLISHED
 [nvcontainer.exe]
  TCP    192.168.1.180:55255    db5sch101101426:https  ESTABLISHED
```

STEP 7 If you want to create a friendlier way of viewing Netstat active connection data, you can pipe the contents to a text file. For example, in the command prompt enter **cd** to take you to the root of the C: drive. Then create a new folder to store the text file with **md activity**, and enter it with **cd activity**.



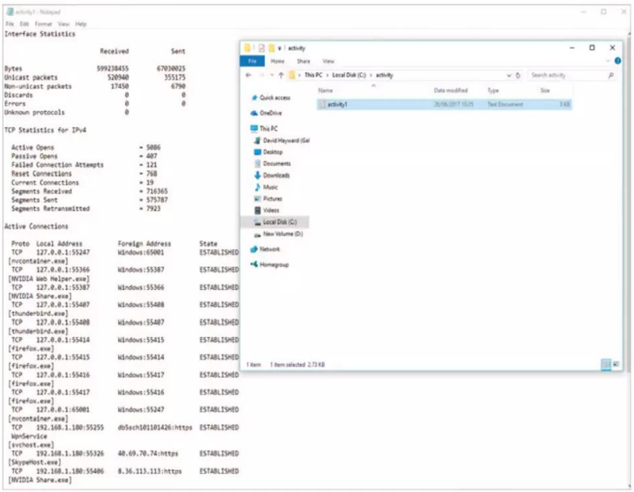
```
C:\Windows\System32>cd\

C:\>md activity

C:\>cd activity

C:\activity>
```

STEP 8 In the activity folder, enter the following: **netstat -e -s -p tcp -b > activity1.txt**. This is the same command as before but this time the output is being sent to a text file, named activity1.txt, rather than outputting to the command prompt window.



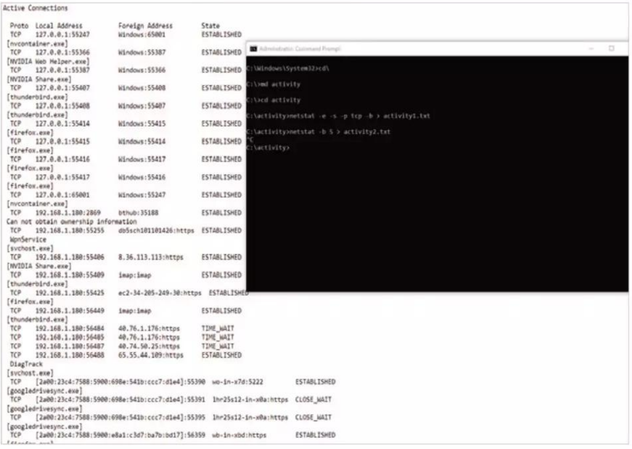
```
C:\Windows\System32>cd\

C:\>md activity

C:\>cd activity

C:\activity>netstat -e -s -p tcp -b > activity1.txt

C:\activity>
```

STEP 9 Using Windows Explorer, locate the C:\activity folder you created and within the activity1.txt file. Double-click the **activity1.txt** file and it opens in Notepad where you're able to view it without the often difficult to read command prompt window.



```
Interface Statistics

                           Received            Sent

Bytes                     599238455        67030025
Unicast packets              520940          355175
Non-unicast packets           17450            6790
Discards                          0               0
Errors                            0               0
Unknown protocols                 0

TCP Statistics for IPv4

  Active Opens                        = 5086
  Passive Opens                       = 407
  Failed Connection Attempts          = 121
  Reset Connections                   = 768
  Current Connections                 = 19
  Segments Received                   = 716365
  Segments Sent                       = 575787
  Segments Retransmitted              = 7923

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:55247        Windows:65001          ESTABLISHED
 [nvcontainer.exe]
  TCP    127.0.0.1:55366        Windows:55387          ESTABLISHED
 [NVIDIA Web Helper.exe]
  TCP    127.0.0.1:55387        Windows:55366          ESTABLISHED
 [NVIDIA Share.exe]
  TCP    127.0.0.1:55407        Windows:55408          ESTABLISHED
 [thunderbird.exe]
  TCP    127.0.0.1:55408        Windows:55407          ESTABLISHED
 [thunderbird.exe]
  TCP    127.0.0.1:55414        Windows:55415          ESTABLISHED
 [firefox.exe]
  TCP    127.0.0.1:55415        Windows:55414          ESTABLISHED
 [firefox.exe]
  TCP    127.0.0.1:55416        Windows:55417          ESTABLISHED
 [firefox.exe]
  TCP    127.0.0.1:55417        Windows:55416          ESTABLISHED
 [firefox.exe]
  TCP    127.0.0.1:65001        Windows:55247          ESTABLISHED
 [nvcontainer.exe]
  TCP    192.168.1.180:55255    db5sch101101426:https  ESTABLISHED
  WpnService
 [svchost.exe]
  TCP    192.168.1.180:55326    40.69.70.74:https      ESTABLISHED
 [SkypeHost.exe]
  TCP    192.168.1.180:55406    8.36.113.113:https     ESTABLISHED
 [NVIDIA Share.exe]
```

STEP 10 If you want to simplify the information and the process, enter: **netstat -b 5 > activity2.txt** into the command prompt within the activity folder on the C: drive. This will record the information and only write the data once you've pressed **Ctrl+C**, which stops the process. Use this for around two minutes to get a record of what's going on.



```
Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:55247        Windows:65001          ESTABLISHED
 [nvcontainer.exe]
  TCP    127.0.0.1:55366        Windows:55387          ESTABLISHED
 [NVIDIA Web Helper.exe]
  TCP    127.0.0.1:55387        Windows:55366          ESTABLISHED
 [NVIDIA Share.exe]
  TCP    127.0.0.1:55407        Windows:55408          ESTABLISHED
 [thunderbird.exe]
  TCP    127.0.0.1:55408        Windows:55407          ESTABLISHED
 [thunderbird.exe]
  TCP    127.0.0.1:55414        Windows:55415          ESTABLISHED
 [firefox.exe]
  TCP    127.0.0.1:55415        Windows:55414          ESTABLISHED
 [firefox.exe]
  TCP    127.0.0.1:55416        Windows:55417          ESTABLISHED
 [firefox.exe]
  TCP    127.0.0.1:55417        Windows:55416          ESTABLISHED
 [firefox.exe]
  TCP    127.0.0.1:65001        Windows:55247          ESTABLISHED
 [nvcontainer.exe]
  TCP    192.168.1.180:2869     bthub:35188            ESTABLISHED
 Can not obtain ownership information
  TCP    192.168.1.180:55255    db5sch101101426:https  ESTABLISHED
  WpnService
 [svchost.exe]
  TCP    192.168.1.180:55406    8.36.113.113:https     ESTABLISHED
 [NVIDIA Share.exe]
  TCP    192.168.1.180:55409    imap:imap              ESTABLISHED
 [thunderbird.exe]
  TCP    192.168.1.180:55425    ec2-34-205-249-30:https  ESTABLISHED
 [firefox.exe]
  TCP    192.168.1.180:56449    imap:imap              ESTABLISHED
 [thunderbird.exe]
  TCP    192.168.1.180:56484    40.76.1.176:https      TIME_WAIT
  TCP    192.168.1.180:56485    40.76.1.176:https      TIME_WAIT
  TCP    192.168.1.180:56487    40.74.50.25:https      TIME_WAIT
  TCP    192.168.1.180:56488    65.55.44.109:https     ESTABLISHED
  DiagTrack
 [svchost.exe]
  TCP    [2a00:23c4:7588:5900:698e:541b:ccc7:d1e4]:55390  wo-in-x7d:5222         ESTABLISHED
 [googledrivesync.exe]
  TCP    [2a00:23c4:7588:5900:698e:541b:ccc7:d1e4]:55391  lhr25s12-in-x0a:https  CLOSE_WAIT
 [googledrivesync.exe]
  TCP    [2a00:23c4:7588:5900:698e:541b:ccc7:d1e4]:55395  lhr25s12-in-x0a:https  CLOSE_WAIT
 [googledrivesync.exe]
  TCP    [2a00:23c4:7588:5900:e8a1:c3d7:ba7b:bd17]:56359  wb-in-xbd:https        ESTABLISHED
```

```
C:\Windows\System32>cd\

C:\>md activity

C:\>cd activity

C:\activity>netstat -e -s -p tcp -b > activity1.txt

C:\activity>netstat -b 5 > activity2.txt
^C
C:\activity>
```

What is a Firewall?

The data packets that come and go between your PC and the outside world can be defined by a set of rules. These rules state whether a packet has access to the system in the first place, then whether or not it can gain access to its destination program. Collectively, these rules make up a Firewall.

Great Walls of Fire

The term firewall comes from fire prevention, where a physical wall is constructed in order to halt the spread of a fire. In digital terms, the physical wall stops malware and other threats from spreading into the system.

Some form of digital protection against unwanted entry into a system has existed for many years but the more recent software side of a firewall, one that we're reasonably familiar with, has only been around since the '80s.

Prior to the modern firewall, system administrators blocked unwanted access through various stages of hardware layers. Long lists of allowed computer addresses were painstakingly entered into mainframes and routers, where programmable chips filtered the white list and simply stopped all access to addresses that weren't on the list; think of a nightclub bouncer, if your name's not on the list you're not getting in.

In its simplest guise, a firewall will look to a defined set of rules then apply those rules to any data packets that pass through it. For example, if you've created a rule whereby all Telnet traffic is blocked, any packet that's trying to reach port 23, the port that Telnet applications listen on for data, will be blocked. While suitably effective this low-level packet filtering does have its Achilles heel, in that it treats each packet as an independent piece of data: not knowing whether it's a part of an already established stream of data. This can be targeted by hackers who want access to a system with a firewall in place. The clever hacker is able to spoof a packet and thus tricking the firewall into letting it pass. It takes some time, and it's a bit hit and miss, but most hackers have plenty of patience when it comes to getting into a network. Therefore a much needed higher degree of firewall monitoring is called for.

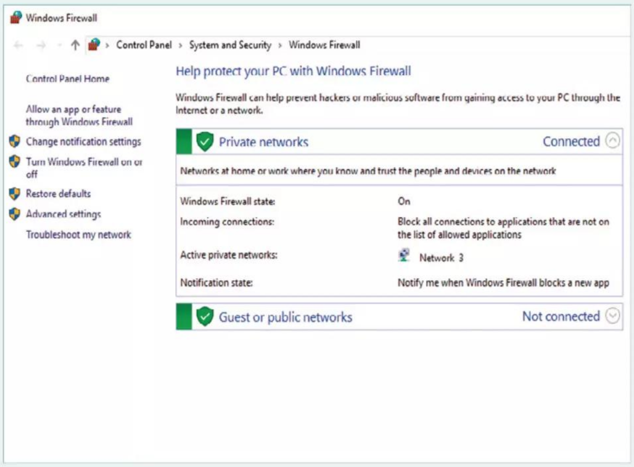
Stateful Inspection firewalls were introduced in the mid '90s and enabled a firewall to log all the connection that passed through it determining what was the start of a new packet stream, part of an existing packet stream or something random. This allows a firewall to allow or drop any access based on a data packet's history. In terms of effectiveness, this makes the firewall more efficient and faster at dealing with connection requests as it doesn't need to continually analyse each packet as an individual but rather as a whole stream. For added layers of protection, if a packet doesn't match any of the connection histories, then it can be evaluated and filtered through the various rules to determine its legitimacy.

A further layer of protection was included into the basic firewall early in the 2000s. Application-layer analysis enabled firewalls to inspect packets that were targeting individual applications within the operating system. Each program or application installed in the system will use a set of protocols to communicate with the outside world. When an application is installed, on a Windows 10 system for example, the installation mechanism will automatically add an instance of it to the Windows 10 firewall. This means that it is able to send and receive information successfully through the Windows firewall without any of it being blocked. By blocking an application's access to the outside world, the user could miss out on regular updates, fixes, patches and so on. One of the key benefits to an application-layer firewall is that it's excellent at blocking specific content, such as known malware and viruses or dangerous websites. It's also capable of determining when a particular protocol is being misused by a rogue application.

Where the firewall proceeds from this point is unclear. However many experts agree that although we'll always need a firewall, the modern systems, networks and devices have so many potential access points that it's fast becoming less efficient to run the standard firewall model. In effect, the modern firewall, regardless of how complex and efficient it has become over the years, is quick becoming a bottle-neck for the operating system. What some experts are theorising is that at some point in the future, the need for a single, overall firewall will be outdated and that the next-generation operating systems will require each program and application that can be installed to act as its own firewall. Whether this will come about is pure fantasy at the moment but at the speed digital technologies grow and evolve there's a good chance of finding out soon enough.

> *Hardware firewalls are an early example of network security*

LAN
WAN
USB
CONSOLE
POWER
RESET


Windows Firewall
Control Panel › System and Security › Windows Firewall
Control Panel Home
Allow an app or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network

Help protect your PC with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

Private networks — Connected

Networks at home or work where you know and trust the people and devices on the network

Windows Firewall state: On

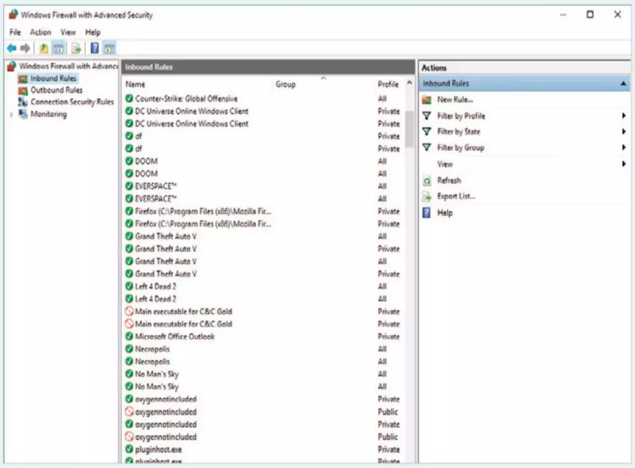
Incoming connections: Block all connections to applications that are not on the list of allowed applications

Active private networks: Network 3

Notification state: Notify me when Windows Firewall blocks a new app

Guest or public networks — Not connected

"The built-in Windows 10 firewall is certainly good enough for most users' needs. It's fast, effective and can be easily configured."

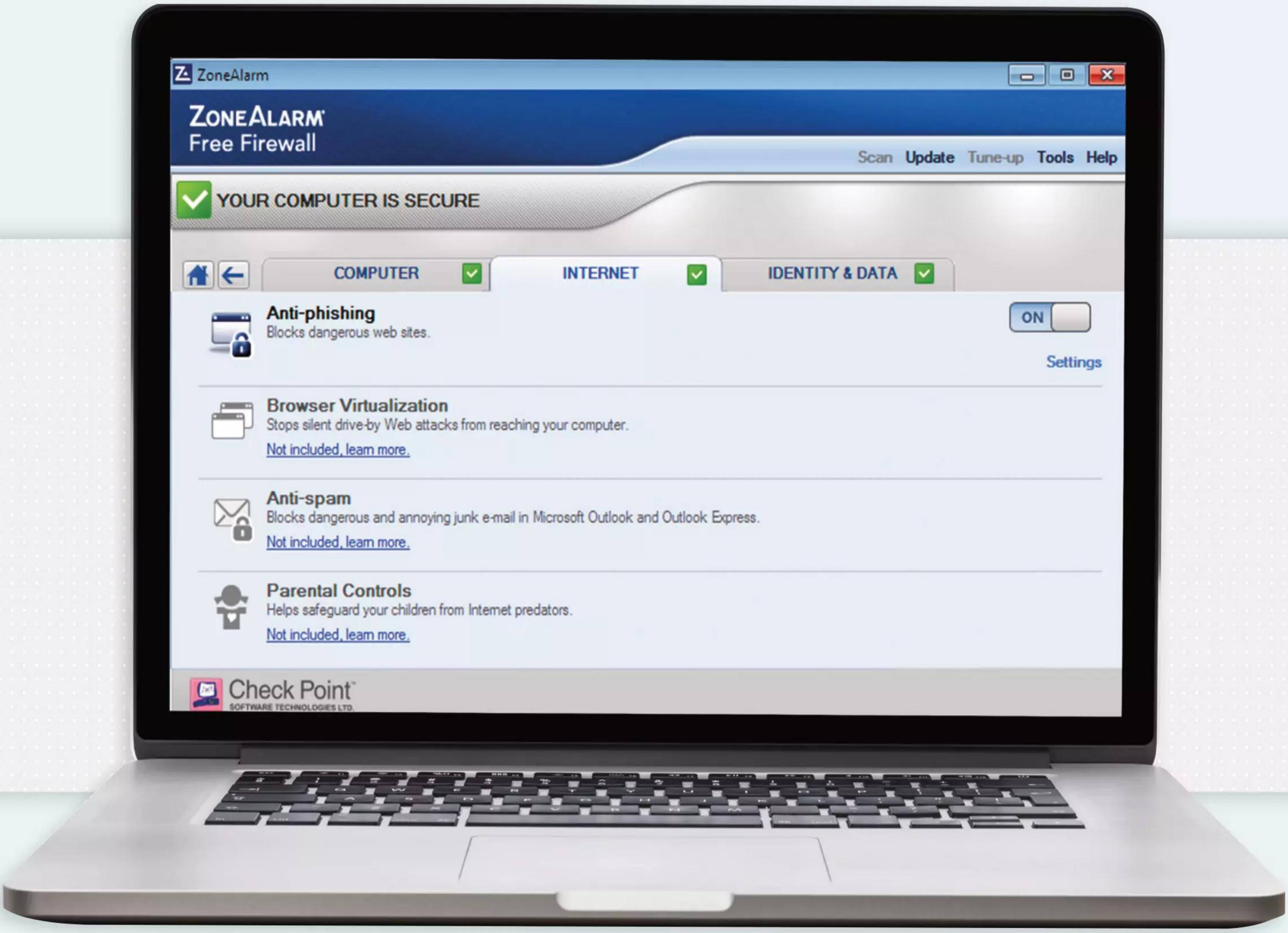

Windows Firewall with Advanced Security
File
Action
View
Help
Windows Firewall with Advance
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Actions
Inbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help

Inbound Rules

Name	Group	Profile
Counter-Strike: Global Offensive		All
DC Universe Online Windows Client		Private
DC Universe Online Windows Client		Private
df		Private
df		Private
DOOM		All
DOOM		All
EVERSPACE™		All
EVERSPACE™		All
Firefox (C:\Program Files (x86)\Mozilla Fir...		Private
Firefox (C:\Program Files (x86)\Mozilla Fir...		Private
Grand Theft Auto V		All
Grand Theft Auto V		Private
Grand Theft Auto V		All
Grand Theft Auto V		Private
Left 4 Dead 2		All
Left 4 Dead 2		All
Main executable for C&C Gold		Private
Main executable for C&C Gold		Private
Microsoft Office Outlook		Private
Necropolis		All
Necropolis		All
No Man's Sky		All
No Man's Sky		All
oxygennotincluded		Private
oxygennotincluded		Public
oxygennotincluded		Private
oxygennotincluded		Public
pluginhost.exe		Private

"When each program, application, game and so on is installed, it is entered into the Windows 10 firewall so it can communicate with the outside world."

"There are countless freely available third-party firewall clients. Some are very good, others not so much."


ZoneAlarm
ZONEALARM
Free Firewall
Scan
Update
Tune-up
Tools
Help
YOUR COMPUTER IS SECURE
COMPUTER
INTERNET
IDENTITY & DATA
ON
Settings
Not included, learn more.
Check Point
SOFTWARE TECHNOLOGIES LTD.

Anti-phishing
Blocks dangerous web sites.

Browser Virtualization
Stops silent drive-by Web attacks from reaching your computer.

Anti-spam
Blocks dangerous and annoying junk e-mail in Microsoft Outlook and Outlook Express.

Parental Controls
Helps safeguard your children from Internet predators.

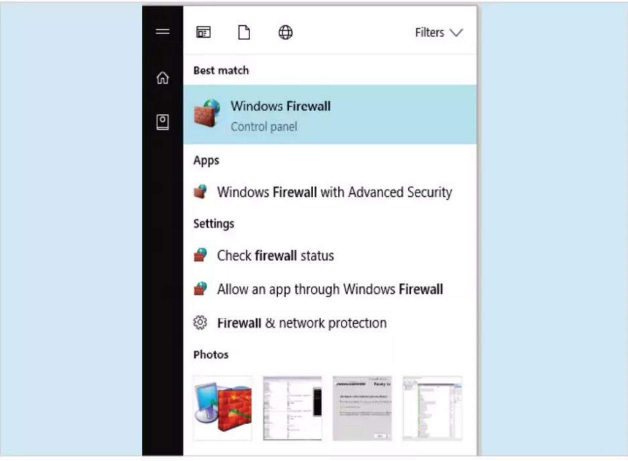
Improving the Windows 10 Firewall

The built-in Windows 10 firewall is a surprisingly good security application. Whilst it may not be as efficient as something offered by one of the third-party security suites, it's certainly more than adequate for the average user.

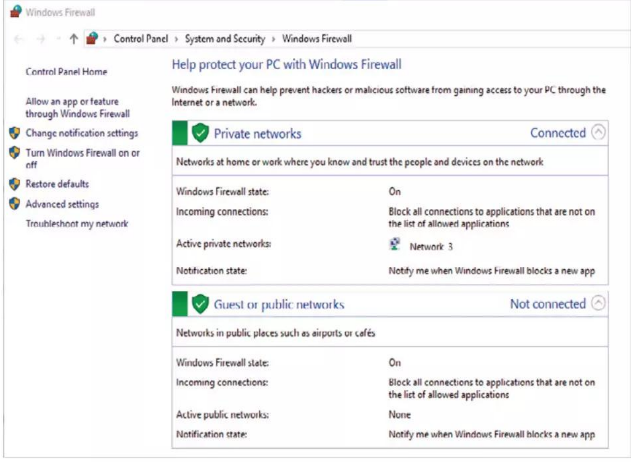
Getting to Know Your Firewall

Generally, there's little need to ever configure the Windows 10 firewall. However, getting to know how it works and improving it is part of being more security-conscious. Here's some tips on how to manage it better.

STEP 1 You can open the main Windows 10 firewall console window by clicking on the Windows Start button and entering firewall into the search box. Click the returned link, Windows Firewall Control Panel, to launch it.


Filters
Best match
Windows Firewall
Control panel
Apps
Windows Firewall with Advanced Security
Settings
Check firewall status
Allow an app through Windows Firewall
Firewall & network protection
Photos

STEP 2 The Windows 10 firewall console window starts by detailing the basic status of the firewall. It should be On by default, unless you've installed a third-party security suite which contains its own firewall. There are two kinds of network listed, Private and Public. Private is for home or work, whereas Public is for cafés and the like.


Windows Firewall
Control Panel › System and Security › Windows Firewall
Control Panel Home
Allow an app or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network

Help protect your PC with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

Private networks — Connected

Networks at home or work where you know and trust the people and devices on the network

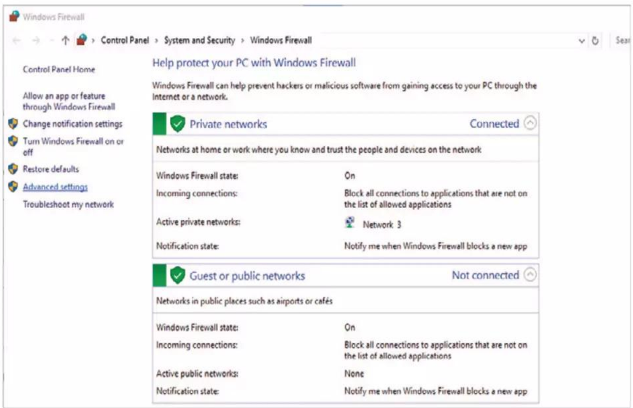
Windows Firewall state: On
Incoming connections: Block all connections to applications that are not on the list of allowed applications
Active private networks: Network 3
Notification state: Notify me when Windows Firewall blocks a new app

Guest or public networks — Not connected

Networks in public places such as airports or cafés

Windows Firewall state: On
Incoming connections: Block all connections to applications that are not on the list of allowed applications
Active public networks: None
Notification state: Notify me when Windows Firewall blocks a new app

STEP 3 Down the left-hand side are some links that will help you configure and improve the firewall, as well as turning it on or off (which isn't recommended under any circumstance other than the installation of an improved third-party firewall). To begin with, start by clicking on the Advanced Settings link.


Windows Firewall
Control Panel › System and Security › Windows Firewall
Control Panel Home
Allow an app or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network

Help protect your PC with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

Private networks — Connected

Networks at home or work where you know and trust the people and devices on the network

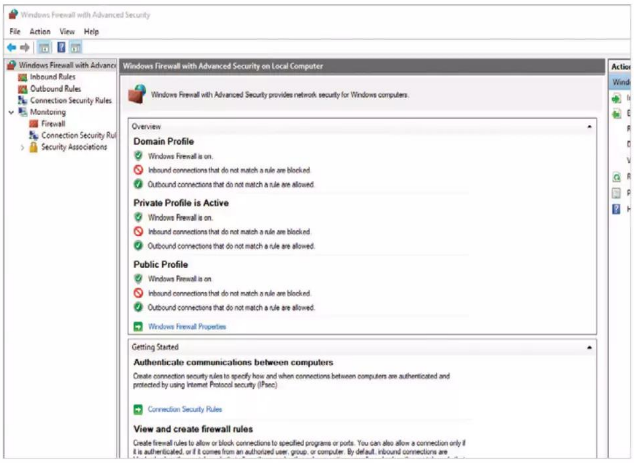
Windows Firewall state: On
Incoming connections: Block all connections to applications that are not on the list of allowed applications
Active private networks: Network 3
Notification state: Notify me when Windows Firewall blocks a new app

Guest or public networks — Not connected

Networks in public places such as airports or cafés

Windows Firewall state: On
Incoming connections: Block all connections to applications that are not on the list of allowed applications
Active public networks: None
Notification state: Notify me when Windows Firewall blocks a new app

STEP 4 The Advanced Settings link launches a new console window. This new console defines the inbound and outbound rules for the entire system and its installed programs and applications. You can set authentication rules between computers, view and create new firewall rules, view the current firewall policies and even monitor what's being blocked in realtime.


Windows Firewall with Advanced Security
File Action View Help
Windows Firewall with Advanc
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Firewall
Connection Security Rul
Security Associations
Windows Firewall with Advanced Security on Local Computer
Actio
Overview
Getting Started

Windows Firewall with Advanced Security provides network security for Windows computers.

Domain Profile
Windows Firewall is on.
Inbound connections that do not match a rule are blocked.
Outbound connections that do not match a rule are allowed.

Private Profile is Active
Windows Firewall is on.
Inbound connections that do not match a rule are blocked.
Outbound connections that do not match a rule are allowed.

Public Profile
Windows Firewall is on.
Inbound connections that do not match a rule are blocked.
Outbound connections that do not match a rule are allowed.

Windows Firewall Properties

Authenticate communications between computers

Create connection security rules to specify how and when connections between computers are authenticated and protected by using Internet Protocol security (IPsec).

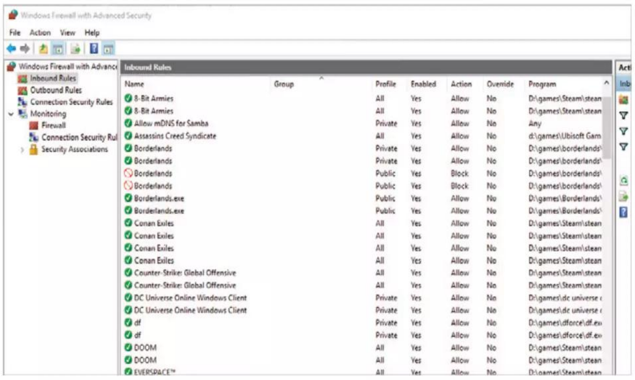
Connection Security Rules

View and create firewall rules

Create firewall rules to allow or block connections to specified programs or ports. You can also allow a connection only if it is authenticated, or if it comes from an authorized user, group, or computer. By default, inbound connections are

STEP 5

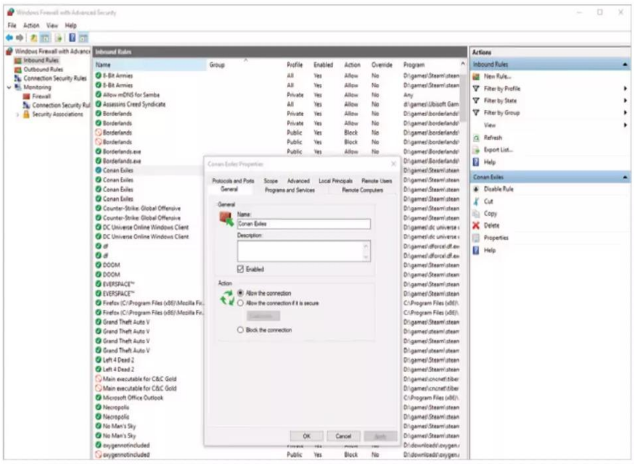
Click on Inbound Rules to the right-hand side of the main console window. This will list the current rules that allow traffic into your computer and to the applications that require it. For example, in this screenshot there are rules for various games that allow multiplayer interaction and the ability to 'talk' to the game server as well as install updates.


Windows Firewall with Advanced Security
File Action View Help
Windows Firewall with Advanced Security
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Firewall
Connection Security Rul
Security Associations
Inbound Rules
Acti

Name	Group	Profile	Enabled	Action	Override	Program
8-Bit Armies		All	Yes	Allow	No	D:\games\Steam\stean
8-Bit Armies		All	Yes	Allow	No	D:\games\Steam\stean
Allow mDNS for Samba		Private	Yes	Allow	No	Any
Assassins Creed Syndicate		All	Yes	Allow	No	d:\games\Ubisoft Gam
Borderlands		Private	Yes	Allow	No	D:\games\borderlands\
Borderlands		Private	Yes	Allow	No	D:\games\borderlands\
Borderlands		Public	Yes	Block	No	D:\games\borderlands\
Borderlands		Public	Yes	Block	No	D:\games\borderlands\
Borderlands.exe		Public	Yes	Allow	No	D:\games\Borderlands\
Borderlands.exe		Public	Yes	Allow	No	D:\games\Borderlands\
Conan Exiles		All	Yes	Allow	No	D:\games\Steam\stean
Conan Exiles		All	Yes	Allow	No	D:\games\Steam\stean
Conan Exiles		All	Yes	Allow	No	D:\games\Steam\stean
Conan Exiles		All	Yes	Allow	No	D:\games\Steam\stean
Counter-Strike: Global Offensive		All	Yes	Allow	No	D:\games\Steam\stean
Counter-Strike: Global Offensive		All	Yes	Allow	No	D:\games\Steam\stean
DC Universe Online Windows Client		Private	Yes	Allow	No	D:\games\dc universe (
DC Universe Online Windows Client		Private	Yes	Allow	No	D:\games\dc universe (
df		Private	Yes	Allow	No	D:\games\dforce\df.ex
df		Private	Yes	Allow	No	D:\games\dforce\df.ex
DOOM		All	Yes	Allow	No	D:\games\Steam\stean
DOOM		All	Yes	Allow	No	D:\games\Steam\stean
EVERSPACE™		All	Yes	Allow	No	D:\games\Steam\stean

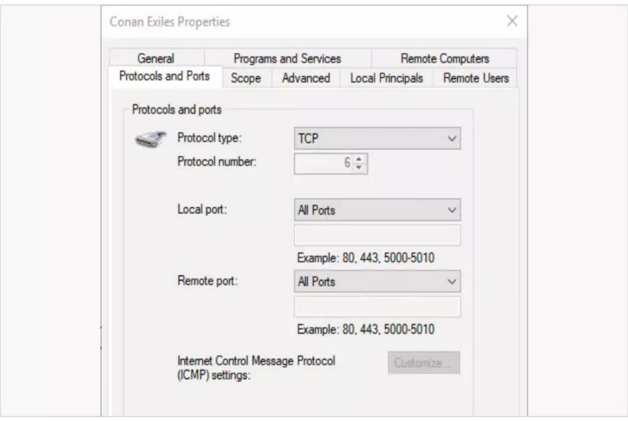
STEP 6

These rules are automatically entered into the firewall when you install the program, game or app. When you install a program you're required to accept and authenticate the process, clicking on Yes to start the installation. This level of administrative access also allows entry of the program into the firewall. Pick one of the entries and double-click it.



STEP 7

The properties of each firewall entry allow a greater degree of control for that particular program. You can change the name of the entry, allow or block the connection, define the physical location of the program on your computer, allow access to the program from remote computers, set the protocol and port number it uses and even which network controller to use.


Conan Exiles Properties
General
Programs and Services
Remote Computers
Protocols and Ports
Scope
Advanced
Local Principals
Remote Users
Protocols and ports
Customize...

Protocol type: TCP

Protocol number: 6

Local port: All Ports

Example: 80, 443, 5000-5010

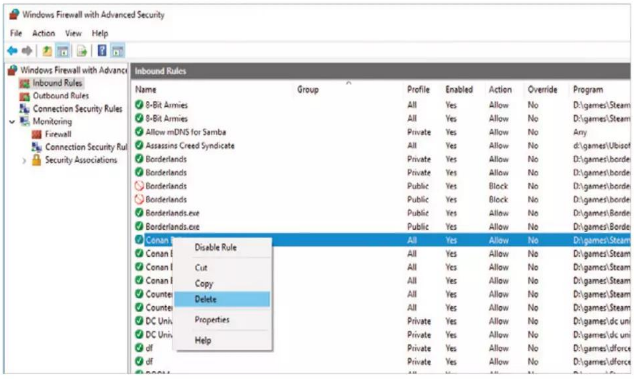
Remote port: All Ports

Example: 80, 443, 5000-5010

Internet Control Message Protocol (ICMP) settings:

STEP 8

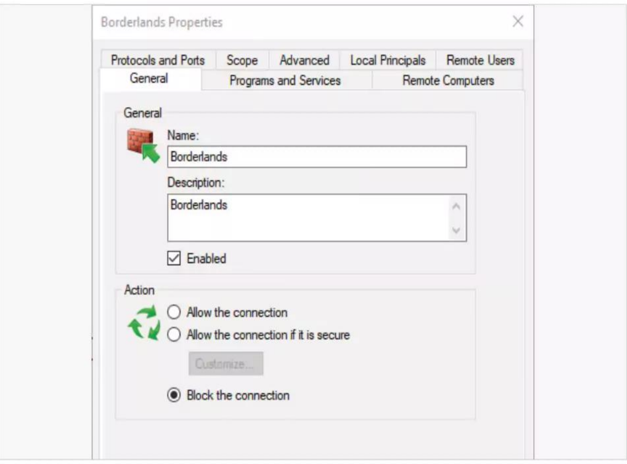
Sometimes, uninstalling a program doesn't automatically remove it from the Windows firewall. The exact reasons why are varied but to help improve the efficiency of the Windows firewall, whenever you remove a program from your system, it's worth checking the firewall to see if its entry has been deleted. To delete an entry, right-click then select Delete from the menu.


Windows Firewall with Advanced Security
File Action View Help
Windows Firewall with Advanced Security
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Firewall
Connection Security Rul
Security Associations
Inbound Rules
Disable Rule
Cut
Copy
Delete
Properties
Help

Name	Group	Profile	Enabled	Action	Override	Program
8-Bit Armies		All	Yes	Allow	No	D:\games\Steam
8-Bit Armies		All	Yes	Allow	No	D:\games\Steam
Allow mDNS for Samba		Private	Yes	Allow	No	Any
Assassins Creed Syndicate		All	Yes	Allow	No	d:\games\Ubisof
Borderlands		Private	Yes	Allow	No	D:\games\borde
Borderlands		Private	Yes	Allow	No	D:\games\borde
Borderlands		Public	Yes	Block	No	D:\games\borde
Borderlands		Public	Yes	Block	No	D:\games\borde
Borderlands.exe		Public	Yes	Allow	No	D:\games\Borde
Borderlands.exe		Public	Yes	Allow	No	D:\games\Borde
Conan		All	Yes	Allow	No	D:\games\Steam
Conan E		All	Yes	Allow	No	D:\games\Steam
Conan E		All	Yes	Allow	No	D:\games\Steam
Conan E		All	Yes	Allow	No	D:\games\Steam
Counte		All	Yes	Allow	No	D:\games\Steam
Counte		All	Yes	Allow	No	D:\games\Steam
DC Univ		Private	Yes	Allow	No	D:\games\dc uni
DC Univ		Private	Yes	Allow	No	D:\games\dc uni
df		Private	Yes	Allow	No	D:\games\dforce
df		Private	Yes	Allow	No	D:\games\dforce

STEP 9

You may not want to delete a rule as it could be used later or if you reinstall the program and it fails to recreate the firewall entry. The recommended process then is to block the rule from communicating with the outside world. To do this, double-click the rule and from the General tab click the Block the connection button.


Borderlands Properties
Protocols and Ports
Scope
Advanced
Local Principals
Remote Users
General
Programs and Services
Remote Computers
General
Action
Customize...

Name: Borderlands

Description: Borderlands

☑ Enabled

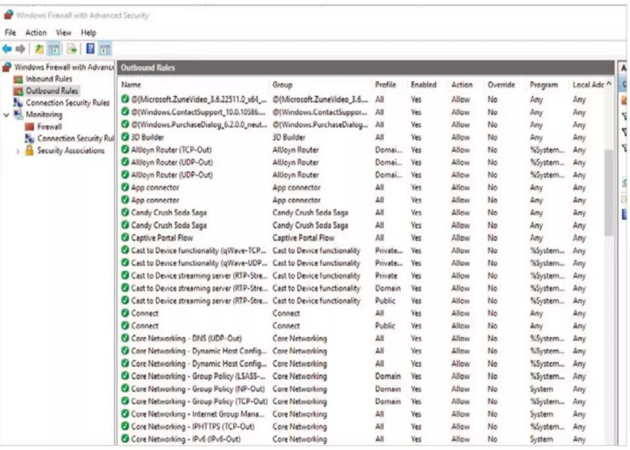
○ Allow the connection

○ Allow the connection if it is secure

● Block the connection

STEP 10

Similarly, the Outbound Rules link will detail the various programs that are allowed to communicate from your computer to an external destination. It's good practise to familiarise yourself with the rules of the firewall, as a rogue program will need to set a rule to communicate. You can then block that rule and stop the threat from reporting back.


Windows Firewall with Advanced Security
File Action View Help
Windows Firewall with Advanc
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Firewall
Connection Security Rul
Security Associations
Outbound Rules

Name	Group	Profile	Enabled	Action	Override	Program	Local Adc
@{Microsoft.ZuneVideo_3.6.22511.0_x64_...	@{Microsoft.ZuneVideo_3.6....	All	Yes	Allow	No	Any	Any
@{Windows.ContactSupport_10.0.10586....	@{Windows.ContactSuppor...	All	Yes	Allow	No	Any	Any
@{Windows.PurchaseDialog_6.2.0.0_neut...	@{Windows.PurchaseDialog...	All	Yes	Allow	No	Any	Any
3D Builder	3D Builder	All	Yes	Allow	No	Any	Any
AllJoyn Router (TCP-Out)	AllJoyn Router	Domai...	Yes	Allow	No	%System...	Any
AllJoyn Router (UDP-Out)	AllJoyn Router	Domai...	Yes	Allow	No	%System...	Any
AllJoyn Router (UDP-Out)	AllJoyn Router	Domai...	Yes	Allow	No	%System...	Any
App connector	App connector	All	Yes	Allow	No	Any	Any
App connector	App connector	All	Yes	Allow	No	Any	Any
Candy Crush Soda Saga	Candy Crush Soda Saga	All	Yes	Allow	No	Any	Any
Candy Crush Soda Saga	Candy Crush Soda Saga	All	Yes	Allow	No	Any	Any
Captive Portal Flow	Captive Portal Flow	All	Yes	Allow	No	Any	Any
Cast to Device functionality (qWave-TCP...	Cast to Device functionality	Private...	Yes	Allow	No	%System...	Any
Cast to Device functionality (qWave-UDP...	Cast to Device functionality	Private...	Yes	Allow	No	%System...	Any
Cast to Device streaming server (RTP-Stre...	Cast to Device functionality	Private	Yes	Allow	No	%System...	Any
Cast to Device streaming server (RTP-Stre...	Cast to Device functionality	Domain	Yes	Allow	No	%System...	Any
Cast to Device streaming server (RTP-Stre...	Cast to Device functionality	Public	Yes	Allow	No	%System...	Any
Connect	Connect	All	Yes	Allow	No	Any	Any
Connect	Connect	Public	Yes	Allow	No	Any	Any
Core Networking - DNS (UDP-Out)	Core Networking	All	Yes	Allow	No	%System...	Any
Core Networking - Dynamic Host Config...	Core Networking	All	Yes	Allow	No	%System...	Any
Core Networking - Dynamic Host Config...	Core Networking	All	Yes	Allow	No	%System...	Any
Core Networking - Group Policy (LSASS-...	Core Networking	Domain	Yes	Allow	No	%System...	Any
Core Networking - Group Policy (NP-Out)	Core Networking	Domain	Yes	Allow	No	System	Any
Core Networking - Group Policy (TCP-Out)	Core Networking	Domain	Yes	Allow	No	%System...	Any
Core Networking - Internet Group Mana...	Core Networking	All	Yes	Allow	No	System	Any
Core Networking - IPHTTPS (TCP-Out)	Core Networking	All	Yes	Allow	No	%System...	Any
Core Networking - IPv6 (IPv6-Out)	Core Networking	All	Yes	Allow	No	System	Any

Creating a Security Plan

A security plan will help you form a better strategy when it comes to tackling your Windows and home network security. A good plan will help keep on top of backups, updates and possible areas of weakness that malware or hackers can exploit.

Plan for the Worst, Hope for the Best

There's a lot to consider when coming up with a good security plan. It's not just a case of occasionally checking for an OS update on your own computer, you have to take into account other computers and the entire network.

An effective security plan should encompass the whole of your network, which includes Windows computers, Android and iOS devices, your router, any powerline adapters, Wi-Fi coverage, access passwords and even where the Ethernet cable runs through.

It may sound a little extreme but like most checklist-type scenarios it can be as in-depth as you like. However, it's worth at least considering some aspects of the home network and overall security before starting a plan.

> *"Users form the most vulnerable point of access for security on any system. Educate and make sure they're safe."*

Users

More than likely the 'user' is the most vulnerable point of access and the biggest security threat to any system or network. Whilst you can have the greatest AV suite and water-tight security system in the world, the user who carelessly visits unbeliveableandobviouslyfakedeals.com is the one that's going to cause you the most headaches. In a home network that's often youngsters, those who don't quite understand the whole Internet security element.

Whilst most youngsters are more tech-savvy than us adults, there's an age range where they'll happily click a link from a friend or something they've seen that looks cool. Therefore take the time to educate and frequently check their accounts or computers for anything suspicious. If possible enforce limits to their browsing and regularly update the browsing rules to make sure they're not going where they shouldn't. Remember, it's not just viruses that a child can download, they could potentially see something that would affect them emotionally.

Updates

Obviously a must-have section of a good security plan is to regularly check for system and program updates. Thankfully, Windows 10 and most security suites will run an automatic check whenever the system is powered up and connected to the Internet. However, there's always some point where an update failed to initialise for some reason or another. Therefore, it's often best to manually check.

Consider too checking for updates for the most frequently used programs. Microsoft Office, GIMP, your browser and even games will inevitably have an update available which can enhance, protect and improve the security of the program. After that, make sure that the other installed programs on the system are up-to-date too, as it's best to make sure there's few weaknesses as possible.

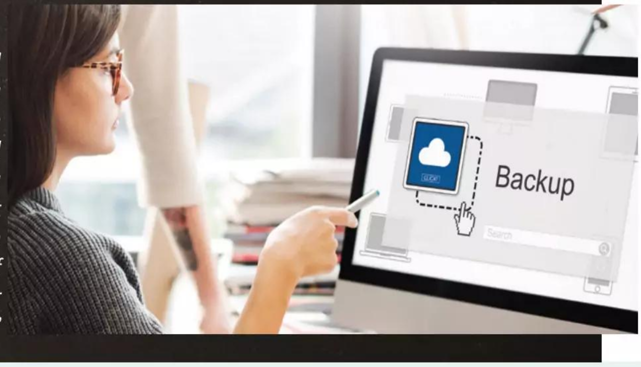
Programs

It can be difficult to keep track of what programs are installed on a system but it's not impossible. If you're serious about the security of your home network and its systems, then taking stock of what programs are installed on each system is worth doing.

Running through a checklist of installed programs you may notice one that shouldn't be there. A quick lookup of the program may reveal that it's a popular backdoor for hackers to get into a system and the attached network. That being the case, it needs to be removed and any firewall entries checked and disabled.

"Router security is vital but it's placement in the home is important too. Not just for effective signal reach but also to stop others from hijacking it."

"Keep all your software up-to-date, including AV suites, programs and the operating system itself."



"Make sure that all the important data is backed up to an external source as well as off site, such as a cloud service. That way if you end up with a complete loss of data, you can recover it easily."

Routers

The family router is the first point of access for anything malicious on the network, since it's the gateway to the outside world. Make sure that the router software is up-to-date and that it's using the best possible wireless security standards and encryption.

It's also beneficial to make sure that the router's admin password and access passwords are hidden from sight. It doesn't take much for someone to look through the front window and make a note of a router password that's carelessly on show for all to see. Consider too, that not all visitors to your home are going to be chivalrous towards viewing your network password.

It's also worth tracking the range of the wireless signal from the router. By installing and using a good Wi-Fi scanner on a mobile device you can tell where the Wi-Fi signal from your router lies beyond your home. Whilst it's good to have a powerful signal, it won't take much for someone to sit nearby with a laptop (or a neighbour) and hack into your network. A Wi-Fi analyser will help you determine the best placement for security and more efficient use of the signal.

Passwords

It's not common for a home user to frequently change their password to the same degree as would an office worker but it's certainly something worth implementing. Using a combination of a good password manager and generator, you can set a 30-day password limit for all users and their access to the sites they visit.

It might sound like an awful lot of hard work on the part of everyone involved but weak passwords and the same password being used across Facebook, banking and gaming is a huge security vulnerability.

Backups

We'll cover backups in a few pages time but for the meantime though making sure that each account and computer is regularly backed up can take much stress out of a security situation. If you're unlucky enough to catch a virus or other malware, or are unfortunate enough to be hacked, you'll need to act quickly to prevent any loss of personal information. This usually means wiping your computer completely.

Having a good and reliable backup solution will help you recover your valuable data in no time, should you ever need to wipe everything or all your data is compromised through malware. It's also worth thinking of investing in a fireproof safe to store your backups along with cloud options for off-site backup security.

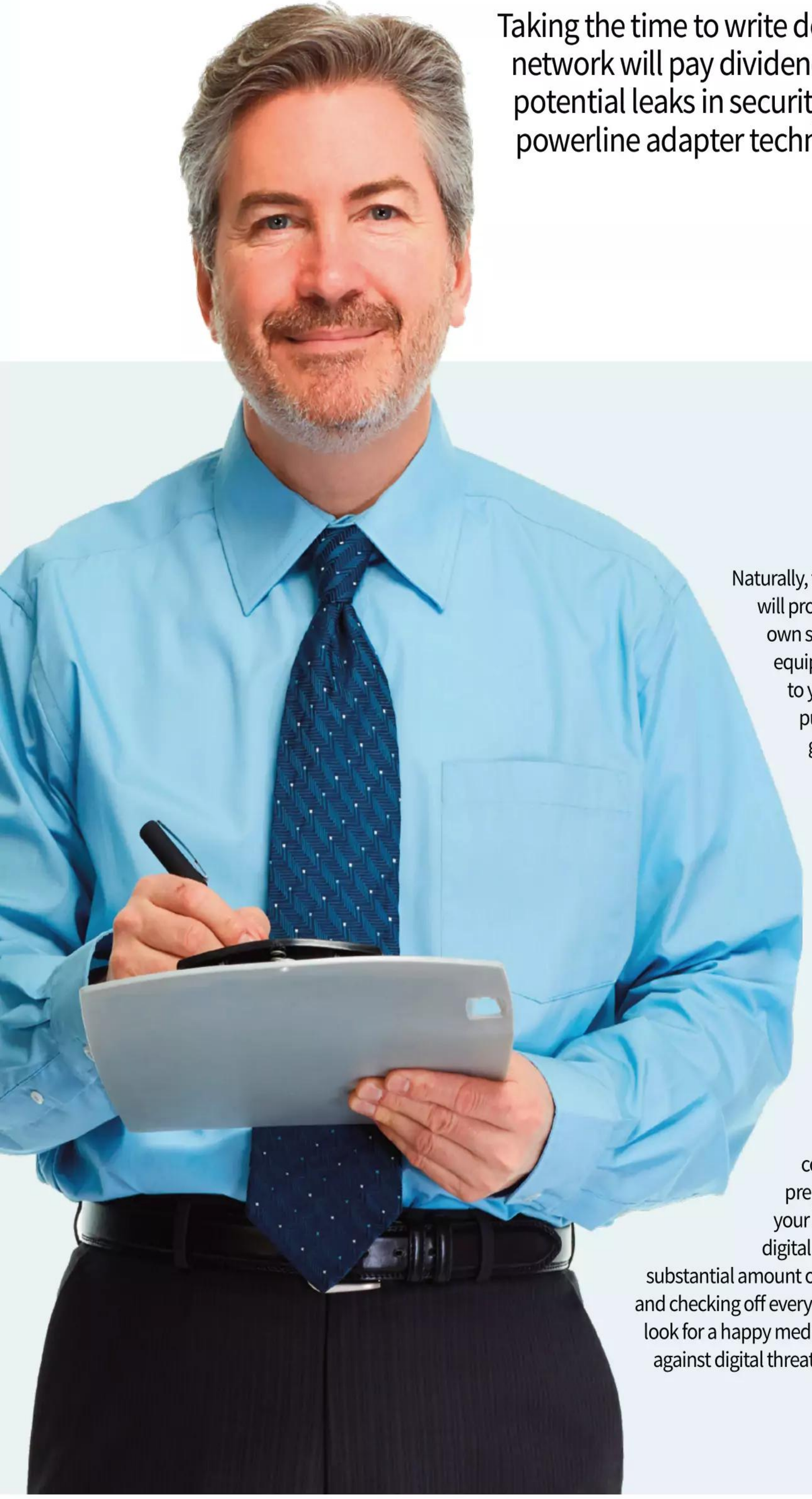
Cabling

It's not always something you need to check but ensuring that the home's Ethernet cabling is secure is an essential element to network security. For example, if you live in shared accommodation, it's possible for a neighbour to be able to be able to connect to your Ethernet cable and steal your bandwidth or gain access to your network resources.

If you can implement all or just some of these elements into your plan, you will be well on the way to making sure that your home network is as secure as possible, without becoming too paranoid over potential threats from outside sources. After all, you lock your doors when you're not at home so why shouldn't you lock your network too.

Windows Security Checklist

Taking the time to write down an effective security plan for your home network will pay dividends in the long run. With it you're able to spot potential leaks in security, secure your home network, Wi-Fi and powerline adapter technologies, and ensure digital peace of mind.



We've come up with a template security checklist that you can use to create your own, for your home network. Remember to tick each section and remember to keep checking regularly and alter it as new devices are added.

> Plan Ahead

Naturally, this is just our example and will probably be different to your own setup and depending on the equipment you have available to you. For the sake of this publication we've taken a more generic approach but it's worth using it as a foundation from which you build your own, personal and unique checklist. Your checklist can be as intricate as you like, detailing specific hardware or software on one or all your computers, devices and so on, that needs to be updated regularly. Just remember though, there is a point where you can become a little too security conscious. Whilst it's great to be prepared for anything, and run your home network like a veritable digital Fort Knox, it can take up a substantial amount of your time applying patches and checking off every item on the list. Therefore, look for a happy medium, whilst remaining vigilant against digital threats.

Checklist

☐ Router

Make sure that your router's admin password and access passwords are in a secure, unviewable place. So visitors can't see them when they come into your home.

☐ Wi-Fi Security

Login in to your router and check that the Wi-Fi is using WPS2. Then check the currently attached devices for any anomalies. If you use any other form of router security, double check it's still functioning as updates can reset routers.

☐ Wireless Positioning

Using a Wi-Fi analyser on your phone or tablet, measure the impact of the wireless signal from the router. If it's reaching out into the street and not so much the rear of the house, then consider moving it. Keep an eye on the signal power and weak locations.

☐ OS Update

Check for any operating system updates on all the computers and Windows mobile devices that connect to the home network.

☐ Security Suite Update

Run a similar update check on any antivirus clients, VPN clients or other third-party security programs and applications.

☐ Program & App Update

Run any update checks on frequently used programs and applications. After that, run as many updates on other installed programs on all your computers.

☐ Installed Rogue Program and App

Check each computer on the network for its list of installed programs. If there's anything in there that doesn't look right, research it and remove it if necessary. Make a note of the programs installed (as a screen shot or physical note) and compare them with each frequent check.

☐ Password Reset

Set a regular, usually 30-day, password reset. Each individual user should be able to reset all their passwords for every site they visit and make sure that the passwords they're using are strong. Use a password manager and password generator if needed.

☐ Firewall Integrity

Check that the firewall on each computer, and potentially any devices, is up and running and that there's no rogue programs within the inbound and outbound rules set.

☐ Backup Important Files

Make sure that each computer and device is regularly backed up. We'll cover how to effectively back up a Windows 10 computer later on. Back up important documents and keep the backup copy somewhere safe; consider purchasing a fireproof safe.

What is a Sandbox?

Sandboxing is an important security technique that's used by companies and individuals the world over. It's not something the average user will normally come across but you can guarantee that every piece of software you use has been sandboxed at some point in its development.

Playing in the Sand

Everyone from software developers and security experts to the hackers themselves will use a sandbox environment to help build and test their products; so what exactly is a sandbox?

Just as the name suggests, a sandbox is a place where you can do something without it affecting the surrounding area: visualise a sandbox in the middle of a garden. In digital security terms, this means a sandbox is a tightly controlled environment that's isolated from the main operating system where a person can test or analyse software and its impact on a virtual system.

The sandbox can be one of a number of implementations: web based, operating system based, program based, network based or even emulating interaction with the Internet. There are countless more examples, each depending on what exactly is being tested and what functions are required to complete the test.

For security, a sandbox is usually an extremely isolated environment that doesn't have access to anything on the company network, or any contact with a host machine. Here the security expert is able to conducts tests on untrusted pieces of code, known malware and viruses and even website content. Should those tests reveal something nasty within, the security expert is able to work their magic and develop a fix that can be further tested and finally deployed to the company's servers, where it's downloaded as updated virus definitions by the security suites and applied to a customer's computer.

Imagine that from the point of view of a hacker, then. The hacker has developed a particularly nasty piece of code that could bring down government agencies and cause widespread panic among the global digital community; they're hardly going to test it on their own computer. They need to create a sandbox environment whereby they can trigger the malware, ransomware or whatever, and let it run its course. In the meantime they can run through various procedures to try and wipe the malware, as a security expert would, to find any weaknesses. Once they've perfected the malware and wiped out any perceivable vulnerabilities, they can then happily upload it to the Internet and sit back as the world is infected with their code.

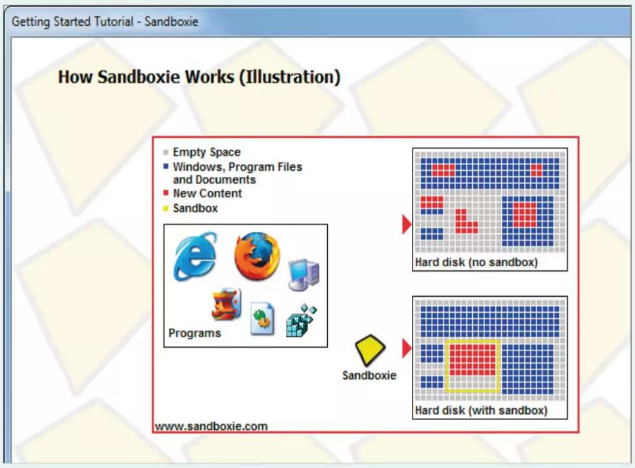
It's not always the testing of malicious code that's associated with sandboxes. For example, the words you're reading now were written using Office 365/Word 2016. Before the product was released by Microsoft, the development team behind Word will have gone through extensive testing, making sure that all the individual components within and that make up Word 2016 all worked. To do so, they will have used a dedicated and separate environment to the one they're using to program on. This specialised environment will have mimicked a real world setup as much as possible, so that when the developer wanted to test something they could compile the code and execute it in an environment that wouldn't affect their normal day-to-day workplace.

The often severe lockdown of a sandbox system does make it difficult to emulate what the average user may be using. The standard desktop computer has many different elements, both hardware and software, that work together to make up the computer that you've customised and personalised. A developer, security expert or software tester can never hope to create something that works 100 percent with every Windows 10 desktop system that's out there.

It's generally accepted then that when testing in a sandbox it's advisable to use as common a hardware and software setup as possible. This way, the developer will likely create a program that works on as high percentage of the computers available. Those computers that differ from the norm, and that may require a little more work for the product to install and work on, can then be dealt with through minor patching and bug testing.

So what's this got to do with you, we hear you say. Well, there are ways in which you can create your own sandbox environment to test in. Consider how many times you've downloaded software from the Internet and executed it without even examining how it may affect your computer. How many times do you visit websites and happily click on whatever message may appear without even reading it properly. With your own sandbox environment, you can download and install a piece of software and see how it runs within a test setup without it ever impacting your real machine. If you get into the habit of testing every bit of software in a sandbox first, you'll certainly be glad should the day come you discover a hidden virus in the folds of an otherwise harmless looking program.

> *“Using a virtual machine as a sandbox is a great way to test programs for every version of Windows, not just the latest”*



Getting Started Tutorial - Sandboxie

How Sandboxie Works (Illustration)

- Empty Space
- Windows, Program Files and Documents
- New Content
- Sandbox

Programs
Sandboxie
Hard disk (no sandbox)
Hard disk (with sandbox)

www.sandboxie.com

"Sandboxie is an environment designed to allow you to test programs without them being installed on your computer."

VirtualBox

"VirtualBox is considered to be one of the leading and easiest to use virtual machines, where you can create a sandbox environment to test in."

Running Windows 10 as a Sandbox

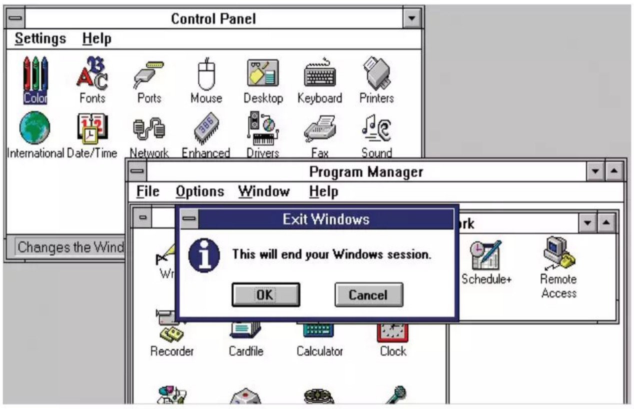
We've already talked about how a sandbox works and essentially what one is in terms of computing and security. However there are many advantages to creating your own virtual sandbox environment. It's not always purely to test suspicious code, as you'll soon discover.

Sand Between Your Toes

If you're still convinced that a sandbox environment can help you out, then read on. We've compiled a list of ten reasons why creating your own Windows 10 sandbox is beneficial to the average user.

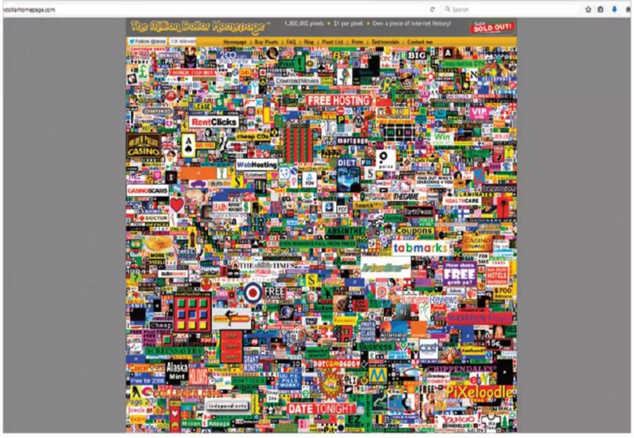
OLD PROGRAMS

Within the Windows 10 virtual sandbox environment you may be able to run older programs that would normally fail, even in compatibility mode, under more modern hardware drivers. Often an older program will look for a specific driver set, if it's too modern then it can fail. Virtual environments use older type drivers by default.


This will end your Windows session.
Control Panel
Settings
Help
Color
Fonts
Ports
Mouse
Desktop
Keyboard
Printers
International
Date/Time
Network
Enhanced
Drivers
Fax
Sound
Changes the Wind
Program Manager
File
Options
Window
Help
Exit Windows
OK
Cancel
Schedule+
Remote Access
Recorder
Cardfile
Calculator
Clock

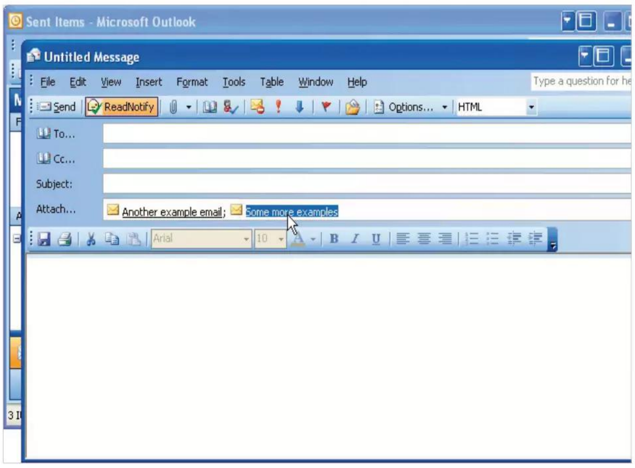
SAFE BROWSING

Within a virtual environment you can browse a site without any of its code being written to the main, host computer. This could simply be cookies and other such relatively harmless additions to sites or it could include data miners and malicious links.


The Million Dollar Homepage
SOLD OUT!
FREE HOSTING
tabmarks
DATE TONIGHT
PiXelogdie

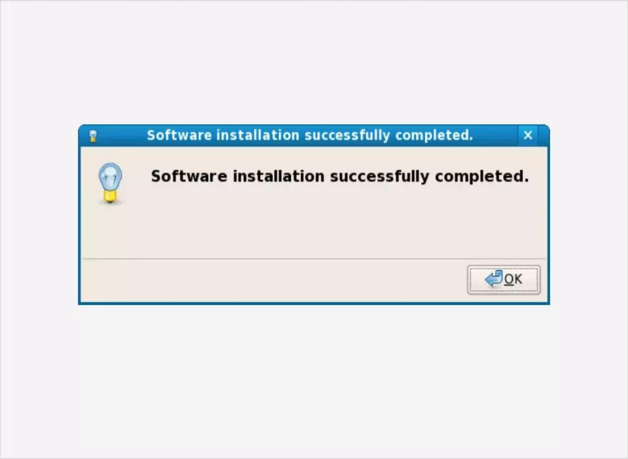
HOST PROTECTION

If you think that a download link or email attachment may contain a virus, then opening it in a safe, virtual environment is the safest bet. Of course, you shouldn't open any unknown email attachments but if you need to, do so in a sandbox. The virus will infect the sandbox and not the host (real) computer.


Attach... Another example email; Some more examples
Sent Items - Microsoft Outlook
Untitled Message
File
Edit
View
Insert
Format
Tools
Table
Window
Help
Type a question for he
Send
ReadNotify
Options...
HTML
To...
Cc...
Subject:
Arial
10

SOFTWARE TESTING

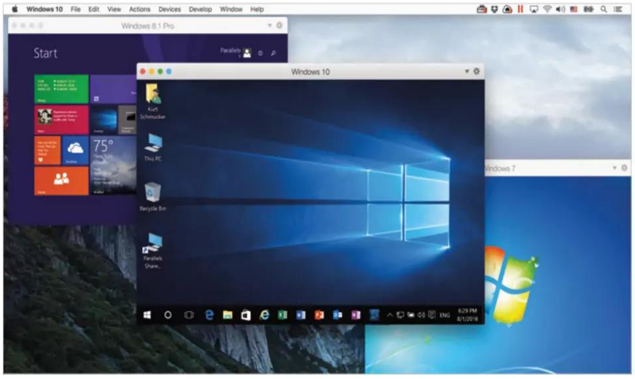
If you're serious about your security and the safety of your home computer, then you should be downloading and installing software in a test environment first before applying it to your real computer. A virtual environment is a great place to see how software works and whether it's worth installing or not.


Software installation successfully completed.

Software installation successfully completed.

VIRTUAL OS

The beauty of a virtual environment, such as one created by VirtualBox, is that you're able to run Windows, macOS and Linux operating systems on top of your host operating system, whatever system that may be. You can install Windows 10 within a virtual environment whilst using Linux or macOS, or vice versa.

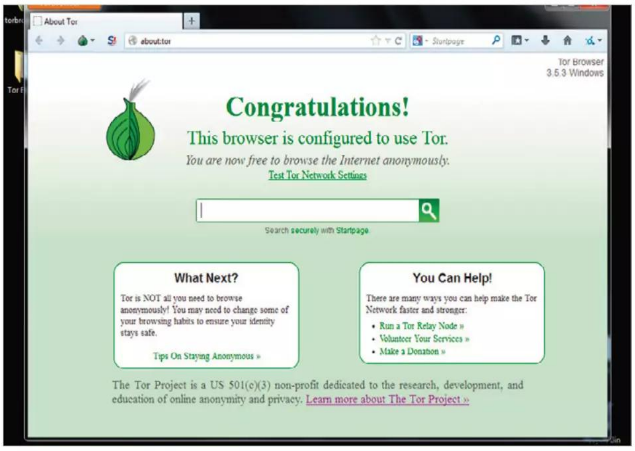


VIRTUAL BACKUP

It is possible to create a virtual copy of a physical machine. This is an excellent way of making sure that the entire machine, that is a snapshot of the OS as it was when copied, is safely backed up and accessible regardless of what operating system you choose to use.

SECURE ANONYMITY

Within a virtual Windows 10 environment you're able to create an anonymity system. By this we mean, you can install a VPN and use the Tor network and surf the Internet without fear of being traced; and what's more, none of it will affect your host operating system.



Congratulations!

This browser is configured to use Tor.

You are now free to browse the Internet anonymously.

Test Tor Network Settings

Search securely with Startpage

What Next?

Tor is NOT all you need to browse anonymously! You may need to change some of your browsing habits to ensure your identity stays safe.

Tips On Staying Anonymous »

You Can Help!

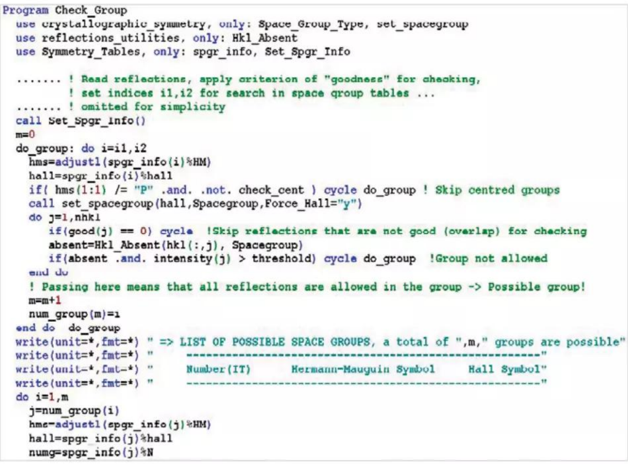
There are many ways you can help make the Tor Network faster and stronger:

- Run a Tor Relay Node »
- Volunteer Your Services »
- Make a Donation »

The Tor Project is a US 501(c)(3) non-profit dedicated to the research, development, and education of online anonymity and privacy. Learn more about The Tor Project »

SAFE DEVELOPMENT

If you're considering developing your own software and apps, then using a virtual environment is an ideal place to test the code as you create it. Should a function you've written have an adverse effect on the OS, then you won't damage your working system.



```
Program Check_Group
  use crystallographic_symmetry, only: Space_Group_Type, set_spacegroup
  use reflections_utilities, only: Hkl_Absent
  use Symmetry_Tables, only: spgr_info, Set_Spgr_Info

  ....... ! Read reflections, apply criterion of "goodness" for checking,
          ! set indices i1,i2 for search in space group tables ...
  ....... ! omitted for simplicity
  call Set_Spgr_Info()
  m=0
  do_group: do i=i1,i2
    hms=adjustl(spgr_info(i)%HM)
    hall=spgr_info(i)%hall
    if( hms(1:1) /= "P" .and. .not. check_cent ) cycle do_group ! Skip centred groups
    call set_spacegroup(hall,Spacegroup,Force_Hall="y")
    do j=1,nhkl
       if(good(j) == 0) cycle  !Skip reflections that are not good (overlap) for checking
       absent=Hkl_Absent(hkl(:,j), Spacegroup)
       if(absent .and. intensity(j) > threshold) cycle do_group  !Group not allowed
    end do
    ! Passing here means that all reflections are allowed in the group -> Possible group!
    m=m+1
    num_group(m)=i
  end do  do_group
  write(unit=*,fmt=*) " => LIST OF POSSIBLE SPACE GROUPS, a total of ",m," groups are possible"
  write(unit=*,fmt=*) "     ------------------------------------------------------"
  write(unit=*,fmt=*) "     Number(IT)      Hermann-Mauguin Symbol     Hall Symbol"
  write(unit=*,fmt=*) "     ------------------------------------------------------"
  do i=1,m
    j=num_group(i)
    hms=adjustl(spgr_info(j)%HM)
    hall=spgr_info(j)%hall
    numg=spgr_info(j)%N
```

FAMILY FRIENDLY

If you have a single-family computer, a virtual environment is a great place for the kids to go without fear of them potentially breaking the system. It doesn't happen often, kids are mostly more tech-savvy than adults but little fingers do have a habit of clicking things they're not supposed to. Virtual environments can be backed up and redeployed easily.

RESTRICTED ACCOUNTS

Again, using children as an example, a virtual child's Windows 10 account can come with all manner of restrictions and monitoring software, to stop them from wandering into the scarier parts of the Internet, such as installing Net Nanny. Again, these controls won't affect the host computer or adult accounts.

Net Nanny

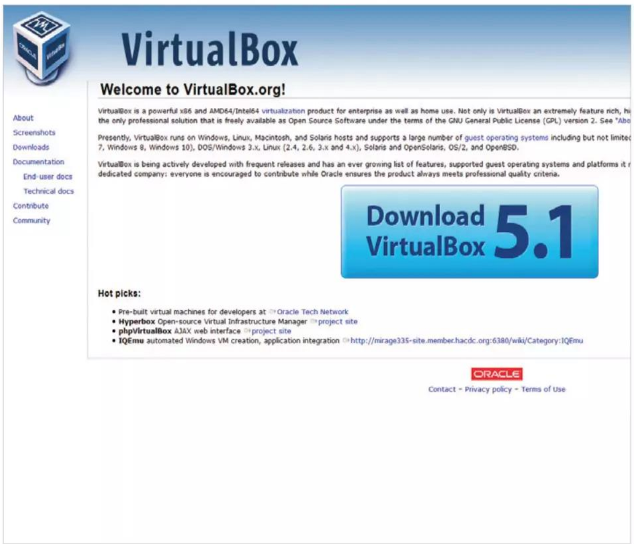
Installing VirtualBox

Oracle's VirtualBox is one of the easiest virtual machine platforms for the beginner to experiment on. Within it you can install Windows, Linux and even macOS for sandbox testing, without ever having to alter your main computer's setup.

Going Virtual

Using a Virtual Machine (VM) will take resources from your computer: memory, hard drive space, processor usage and so on. So make sure you have enough of each before commencing.

STEP 1 The first task is getting hold of VirtualBox. If you haven't already, head over to www.virtualbox.org and click on the large 'Download VirtualBox 5.1' box. This will take you to the main download page. Locate the correct host for your system, Windows or Mac, the Host is the current installed, main operating system, and click to begin the download.



Welcome to VirtualBox.org!

VirtualBox is a powerful x86 and AMD64/Intel64 virtualization product for enterprise as well as home use. Not only is VirtualBox an extremely feature rich, hi
the only professional solution that is freely available as Open Source Software under the terms of the GNU General Public License (GPL) version 2. See "Abo

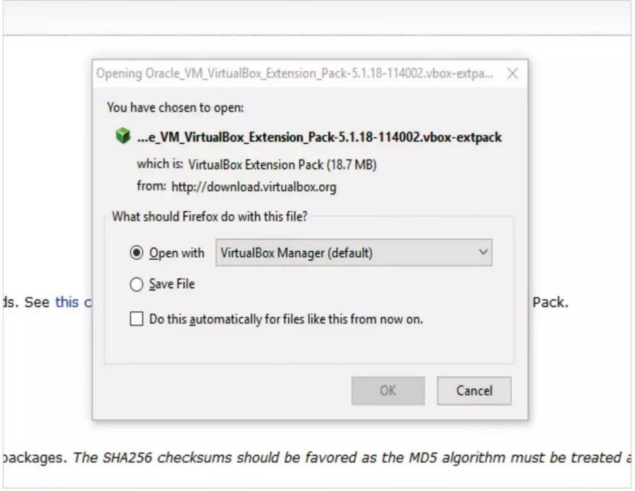
Presently, VirtualBox runs on Windows, Linux, Macintosh, and Solaris hosts and supports a large number of guest operating systems including but not limitec
7, Windows 8, Windows 10), DOS/Windows 3.x, Linux (2.4, 2.6, 3.x and 4.x), Solaris and OpenSolaris, OS/2, and OpenBSD.

VirtualBox is being actively developed with frequent releases and has an ever growing list of features, supported guest operating systems and platforms it r
dedicated company: everyone is encouraged to contribute while Oracle ensures the product always meets professional quality criteria.

Hot picks:

- Pre-built virtual machines for developers at Oracle Tech Network
- **Hyperbox** Open-source Virtual Infrastructure Manager project site
- **phpVirtualBox** AJAX web interface project site
- **IQEmu** automated Windows VM creation, application integration http://mirage335-site.member.hacdc.org:6380/wiki/Category:IQEmu

STEP 2 Next, whilst still at the VirtualBox download page, locate the VirtualBox Extension Pack link. The Extension Pack supports USB devices, as well as numerous other extras that can help make the VM environment a more accurate emulation of a 'real' computer.



Opening Oracle_VM_VirtualBox_Extension_Pack-5.1.18-114002.vbox-extpa...

You have chosen to open:

...e_VM_VirtualBox_Extension_Pack-5.1.18-114002.vbox-extpack

which is: VirtualBox Extension Pack (18.7 MB)

from: http://download.virtualbox.org

What should Firefox do with this file?

● Open with VirtualBox Manager (default)

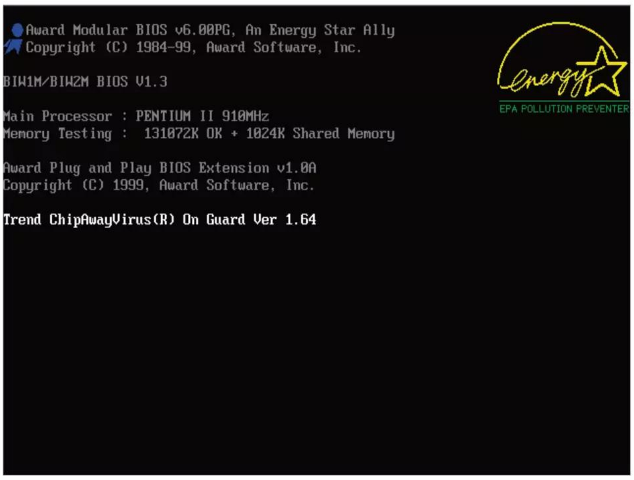
○ Save File

☐ Do this automatically for files like this from now on.

ds. See this c … Pack.

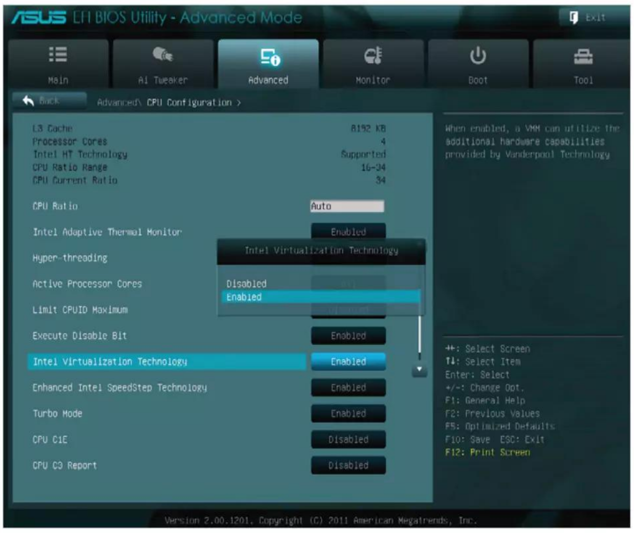
ackages. *The SHA256 checksums should be favored as the MD5 algorithm must be treated a*

STEP 3 With the correct packages downloaded, and before you install anything, you need to make sure that the computer you're using is capable of hosting a VM. To do this, reboot the computer and enter the BIOS. When the computer starts up, press the Del, F2, or whichever key is necessary to Enter Setup.



```
Award Modular BIOS v6.00PG, An Energy Star Ally
Copyright (C) 1984-99, Award Software, Inc.

BIW1M/BIW2M BIOS V1.3

Main Processor : PENTIUM II 910MHz
Memory Testing :  131072K OK + 1024K Shared Memory

Award Plug and Play BIOS Extension v1.0A
Copyright (C) 1999, Award Software, Inc.

Trend ChipAwayVirus(R) On Guard Ver 1.64
```

STEP 4 Each BIOS is laid out differently so it's very difficult to assess where to look in each personal example. However, as a general rule of thumb, you're looking for Intel Virtualisation Technology or simply Virtualisation: usually within the Advanced section of the BIOS. When you've located it, Enable it, save the settings, exit the BIOS and reboot the computer.


ASUS EFI BIOS Utility - Advanced Mode
Exit
Main
Ai Tweaker
Advanced
Monitor
Boot
Tool
Back
Advanced\ CPU Configuration >

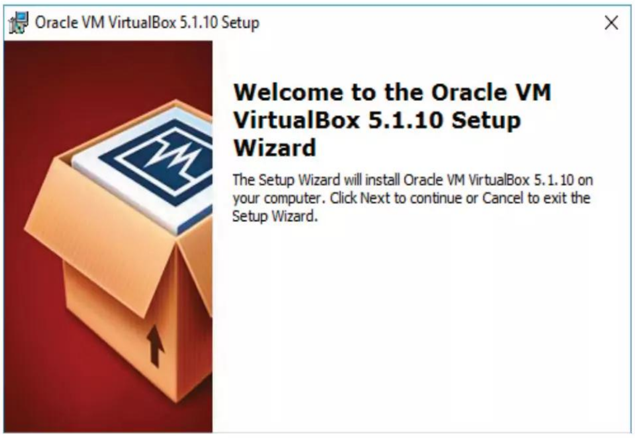
```
L3 Cache                                8192 KB
Processor Cores                               4
Intel HT Technology                   Supported
CPU Ratio Range                           16-34
CPU Current Ratio                            34

CPU Ratio                              Auto

Intel Adaptive Thermal Monitor         Enabled
                     Intel Virtualization Technology
Hyper-threading
                     Disabled
Active Processor Cores
                     Enabled
Limit CPUID Maximum

Execute Disable Bit                    Enabled

Intel Virtualization Technology        Enabled

Enhanced Intel SpeedStep Technology    Enabled

Turbo Mode                             Enabled

CPU C1E                                Disabled

CPU C3 Report                          Disabled
```

When enabled, a VMM can utilize the additional hardware capabilities provided by Vanderpool Technology

```
→←: Select Screen
↑↓: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F2: Previous Values
F5: Optimized Defaults
F10: Save  ESC: Exit
F12: Print Screen
```

Version 2.00.1201. Copyright (C) 2011 American Megatrends, Inc.

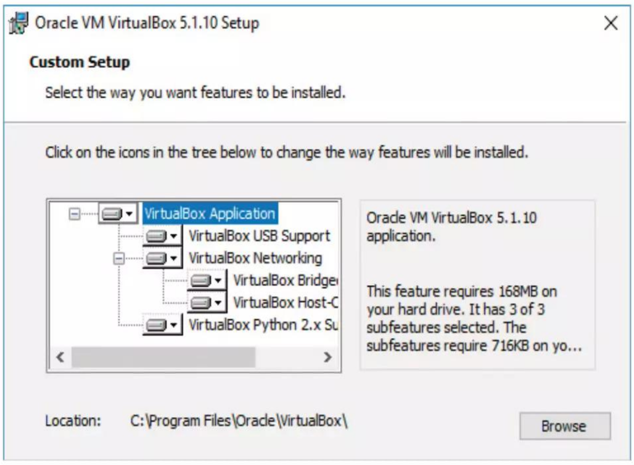
STEP 5 With the computer back up and running, locate the downloaded main VirtualBox application and double-click to begin the installation process. Click Next to continue, when you're ready.


Oracle VM VirtualBox 5.1.10 Setup

Welcome to the Oracle VM VirtualBox 5.1.10 Setup Wizard

The Setup Wizard will install Oracle VM VirtualBox 5.1.10 on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

STEP 6 The default installation location of VirtualBox should satisfy most users but if you have any special location requirements click on the 'Browse' button and change the install folder. Then, make sure that all the icons in the VirtualBox feature tree are selected and none of them has a red X next to them. Click Next to move on.


Oracle VM VirtualBox 5.1.10 Setup
Custom Setup
Select the way you want features to be installed.
VirtualBox Application
VirtualBox USB Support
VirtualBox Networking
VirtualBox Bridge
VirtualBox Host-C
VirtualBox Python 2.x Su
Browse

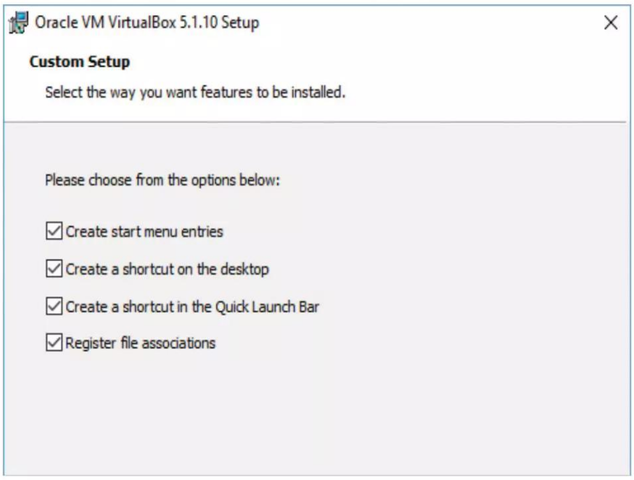
Click on the icons in the tree below to change the way features will be installed.

Oracle VM VirtualBox 5.1.10 application.

This feature requires 168MB on your hard drive. It has 3 of 3 subfeatures selected. The subfeatures require 716KB on yo...

Location: C:\Program Files\Oracle\VirtualBox\

STEP 7 This section can be left alone to the defaults, should you wish. It simply makes life a little easier when dealing with VMs, especially when dealing with downloaded VMs, which you may encounter in the future. Again, clicking Next will move you on to the next stage.


Oracle VM VirtualBox 5.1.10 Setup
Custom Setup
Select the way you want features to be installed.

Please choose from the options below:

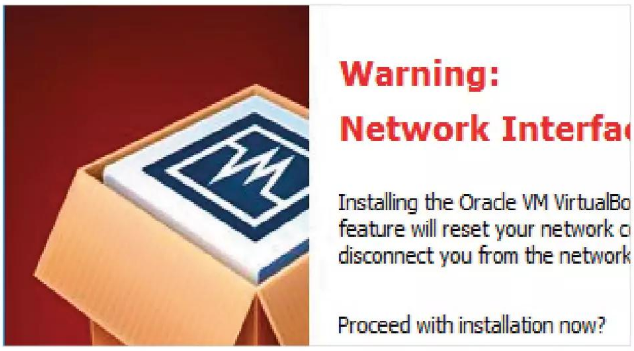
☑ Create start menu entries

☑ Create a shortcut on the desktop

☑ Create a shortcut in the Quick Launch Bar

☑ Register file associations

STEP 8 When installing VirtualBox your network connection will be disabled for a very brief period. This is due to VirtualBox creating a linked, virtual network connection so that any VM installed will be able to access the Internet, and your home network resources, via the computer's already established network connection. Click Yes, then Install to begin the installation.

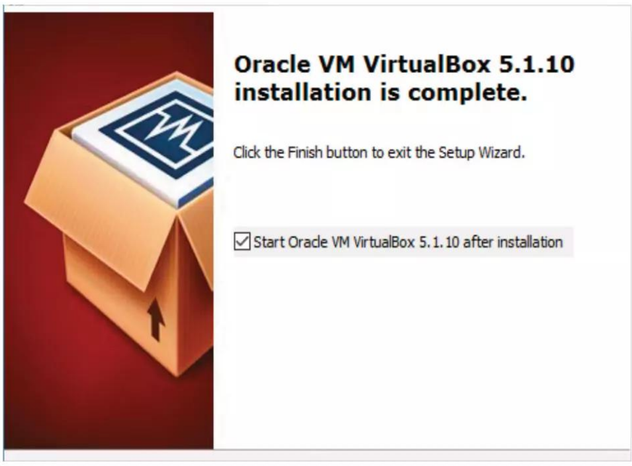


Warning: Network Interfa

Installing the Oracle VM VirtualBo
feature will reset your network c
disconnect you from the network

Proceed with installation now?

STEP 9 You may be asked by Windows to accept a security notification. Click Yes for this and you might encounter a dialogue box asking you to trust the installation from Oracle; again, click yes and accept the installation of the VirtualBox application. When it's complete, click Finish to start VirtualBox.

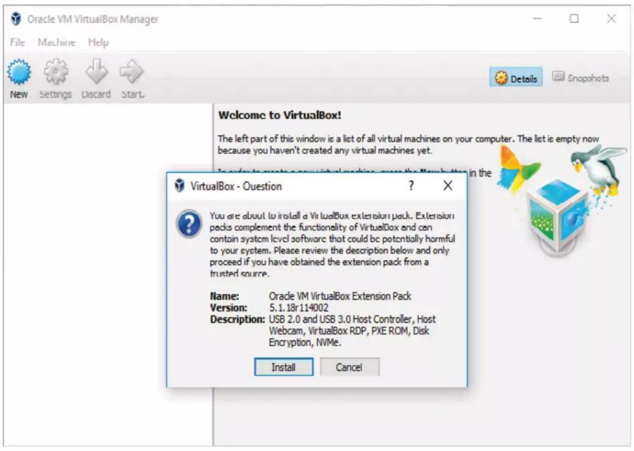


Oracle VM VirtualBox 5.1.10 installation is complete.

Click the Finish button to exit the Setup Wizard.

☑ Start Oracle VM VirtualBox 5.1.10 after installation

STEP 10 With VirtualBox up and running you can now install the VirtualBox Extension Pack. Locate the downloaded add-on and double-click. There may be a short pause whilst VirtualBox analyses the pack but you eventually receive a message to install it; obviously click Install to begin the process, scroll down the next screen to accept the agreement and click I Agree.


Oracle VM VirtualBox Manager
File
Machine
Help
New
Settings
Discard
Start
Details
Snapshots
VirtualBox - Question
Install
Cancel

Welcome to VirtualBox!

The left part of this window is a list of all virtual machines on your computer. The list is empty now because you haven't created any virtual machines yet.

You are about to install a VirtualBox extension pack. Extension packs complement the functionality of VirtualBox and can contain system level software that could be potentially harmful to your system. Please review the description below and only proceed if you have obtained the extension pack from a trusted source.

Name: Oracle VM VirtualBox Extension Pack
Version: 5.1.18r114002
Description: USB 2.0 and USB 3.0 Host Controller, Host Webcam, VirtualBox RDP, PXE ROM, Disk Encryption, NVMe.

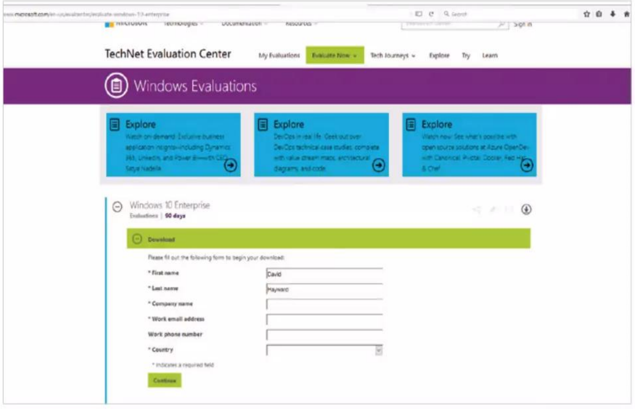
Installing Windows 10 in VirtualBox

Installing Windows 10 within a VM carries with it a clause: you need to make sure you have a valid license. However, if you're testing something then you can use the Windows 10 Enterprise Evaluation image, which will last for 90 days.

Window Installations

Naturally you might own a spare Windows 10 license to use for the VM but for this tutorial we're going for the 90 day Windows 10 Enterprise Evaluation model. To begin with, browse to https://microsoft.com/en-us/evalcenter/evaluate-windows-10-enterprise.

STEP 1 You need to register with Microsoft prior to being able to download the Windows 10 image; simply click the Register button and fill in the required fields. When done, click Continue and choose the ISO Enterprise option, then your language choice and 64-bit, followed by the Continue button once more to begin the download.

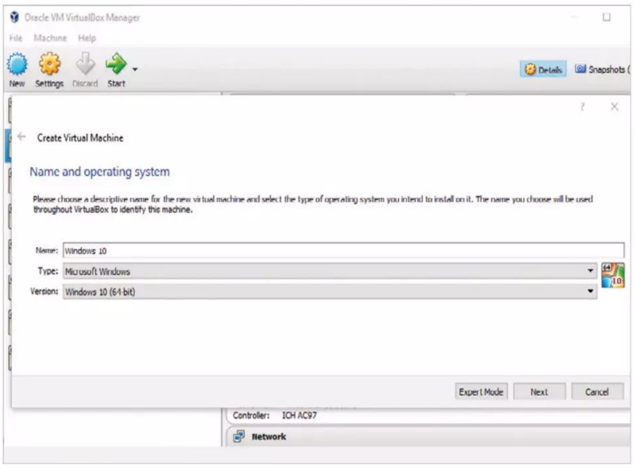

TechNet Evaluation Center
My Evaluations
Evaluate Now
Tech Journeys
Explore
Try
Learn
Windows Evaluations
Explore
Explore
Explore
Windows 10 Enterprise
90 days
Download
Continue

Please fill out the following form to begin your download:

* First name: David
* Last name: Hayward
* Company name:
* Work email address:
Work phone number:
* Country:

* indicates a required field

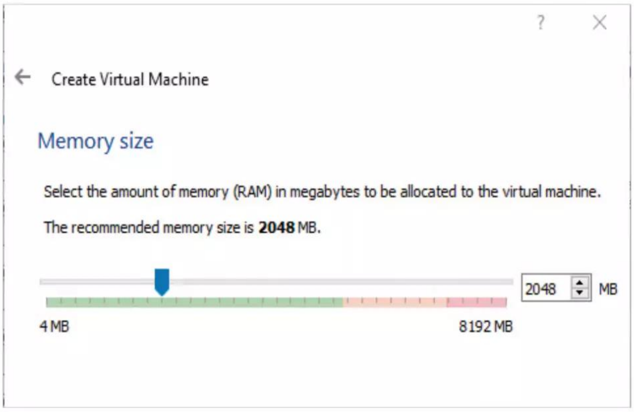
STEP 2 The ISO you're downloading is around 4GB in size, so it may take some time, depending on the speed of your connection. Open VirtualBox and click on the New icon located in the top right of the main VirtualBox window. In the Name field enter Windows 10, this should automatically change the Type and Version fields accordingly. Click Next when ready.


Oracle VM VirtualBox Manager
File
Machine
Help
New
Settings
Discard
Start
Details
Snapshots
Create Virtual Machine
Name and operating system
Expert Mode
Next
Cancel
Controller:
ICH AC97
Network

Please choose a descriptive name for the new virtual machine and select the type of operating system you intend to install on it. The name you choose will be used throughout VirtualBox to identify this machine.

Name: Windows 10
Type: Microsoft Windows
Version: Windows 10 (64-bit)

STEP 3 You need to set an amount of memory from your host computer to use as virtual RAM for the VM. Naturally, you don't want to take too much as your computer will suffer due to low memory when the VM is running. Ideally, you need to allocate around 2GB of memory to the VM. Click Next when ready.

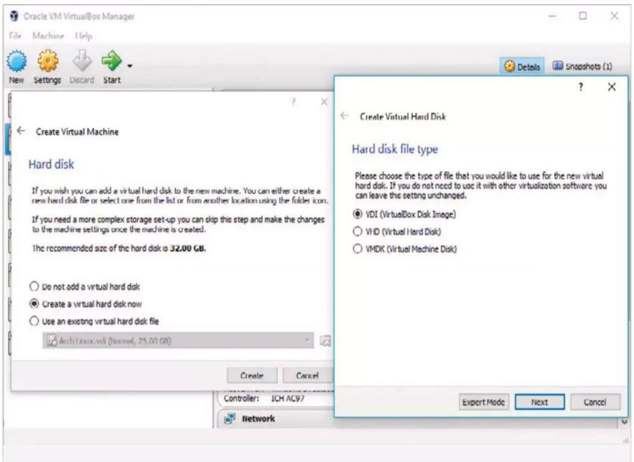

Create Virtual Machine
Memory size
4 MB
8192 MB
MB

Select the amount of memory (RAM) in megabytes to be allocated to the virtual machine.

The recommended memory size is **2048** MB.

2048 MB

STEP 4 The next section will enable you to create a virtual hard disk, in which the Windows 10 virtual machine can be installed. The default option: 'Create a virtual hard disk now' is recommended, then click the Create button to proceed. The pop-up box will detail the type of virtual hard disk; stick to VDI and click Next.


Oracle VM VirtualBox Manager
File
Machine
Help
New
Settings
Discard
Start
Details
Snapshots (1)
Create Virtual Machine
Hard disk
Create
Cancel
Controller:
ICH AC97
Network
Create Virtual Hard Disk
Hard disk file type
Expert Mode
Next
Cancel

If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk file or select one from the list or from another location using the folder icon.

If you need a more complex storage set-up you can skip this step and make the changes to the machine settings once the machine is created.

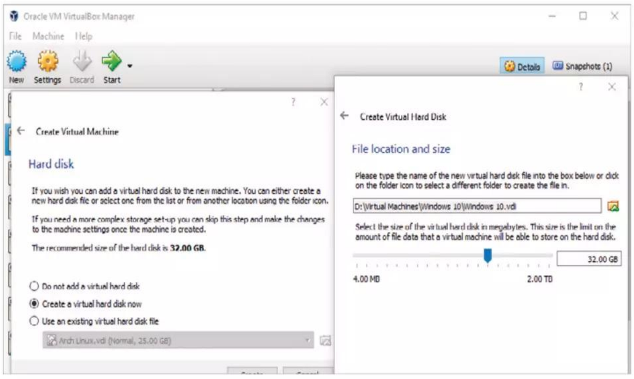
The recommended size of the hard disk is **32.00 GB**.

○ Do not add a virtual hard disk
● Create a virtual hard disk now
○ Use an existing virtual hard disk file

Please choose the type of file that you would like to use for the new virtual hard disk. If you do not need to use it with other virtualization software you can leave this setting unchanged.

● VDI (VirtualBox Disk Image)
○ VHD (Virtual Hard Disk)
○ VMDK (Virtual Machine Disk)

STEP 5 The default Dynamically Allocated option will suffice for this instance, so click Next. VirtualBox recommends that you allocate 32GB of physical hard drive space to creating the virtual hard disk. Make sure your hard drive has enough spare capacity and click the Create button.


Oracle VM VirtualBox Manager
File Machine Help
New Settings Discard Start
Details Snapshots (1)

Create Virtual Machine

Hard disk

If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk file or select one from the list or from another location using the folder icon.

If you need a more complex storage set-up you can skip this step and make the changes to the machine settings once the machine is created.

The recommended size of the hard disk is **32.00 GB**.

○ Do not add a virtual hard disk
● Create a virtual hard disk now
○ Use an existing virtual hard disk file
Arch Linux.vdi (Normal, 25.00 GB)

Create Virtual Hard Disk

File location and size

Please type the name of the new virtual hard disk file into the box below or click on the folder icon to select a different folder to create the file in.

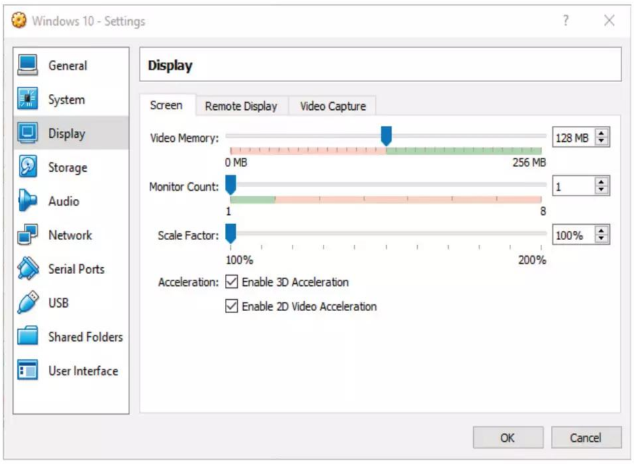
D:\Virtual Machines\Windows 10\Windows 10.vdi

Select the size of the virtual hard disk in megabytes. This size is the limit on the amount of file data that a virtual machine will be able to store on the hard disk.

32.00 GB

4.00 MB
2.00 TB

STEP 6 The Windows 10 VM is now listed in the available VMs in VirtualBox. Before you begin to install it though, click on the Settings icon whilst the Windows 10 VM is highlighted. In the General tab, click Advanced and enable Bidirectional for Shared Clipboard and Drag 'n' Drop. In Display, enable 3D and 2D Video Acceleration. Click OK to finish.


Windows 10 - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Display
Screen
Remote Display
Video Capture
0 MB
256 MB
1
8
100%
200%
OK
Cancel

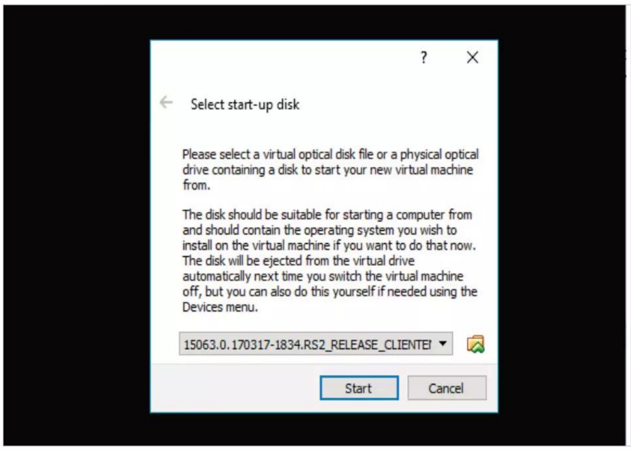
Video Memory: 128 MB

Monitor Count: 1

Scale Factor: 100%

Acceleration: ☑ Enable 3D Acceleration
☑ Enable 2D Video Acceleration

STEP 7 With the Settings console window closed, and the VM highlighted, click on the Start button. This will open a new window, asking for the location of the Windows 10 ISO you downloaded from the Microsoft site in the first few steps. Use the folder icon to locate the ISO and click Open, then the Start button to commence the installation.


Select start-up disk

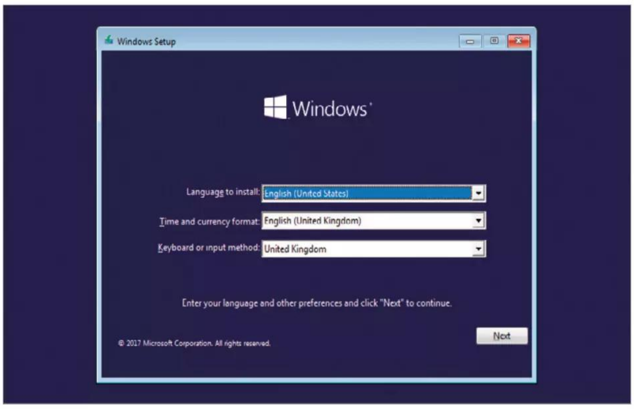
Please select a virtual optical disk file or a physical optical drive containing a disk to start your new virtual machine from.

The disk should be suitable for starting a computer from and should contain the operating system you wish to install on the virtual machine if you want to do that now. The disk will be ejected from the virtual drive automatically next time you switch the virtual machine off, but you can also do this yourself if needed using the Devices menu.

15063.0.170317-1834.RS2_RELEASE_CLIENTEI

Start
Cancel

STEP 8 The Windows ISO will now load, and begin the installation process. The first options you need to set are the language, time and keyboard. Set your preferences, although the default is English US to begin with, and click on the Next button when you're ready to continue.


Windows Setup
Windows
Next

Language to install: English (United States)

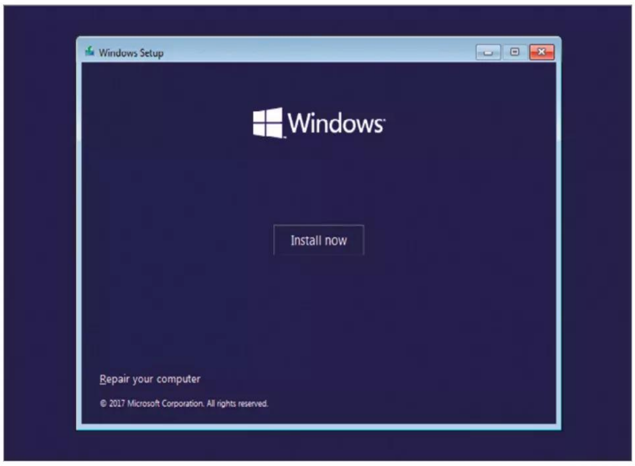
Time and currency format: English (United Kingdom)

Keyboard or input method: United Kingdom

Enter your language and other preferences and click "Next" to continue.

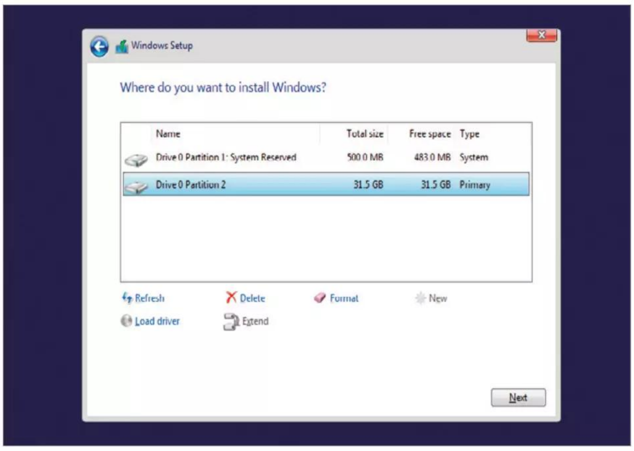
© 2017 Microsoft Corporation. All rights reserved.

STEP 9 You now have an Install Now option available. Click it to begin the installation, then tick the license agreement box followed by Next. There are two possible options to install Windows 10, Upgrade and Custom. Since this is a blank hard drive, the Custom option is the only viable mode. Click it to continue.


Windows Setup
Windows
Install now
Repair your computer

© 2017 Microsoft Corporation. All rights reserved.

STEP 10 The drive available will be the 32GB virtual hard disk you created. Click on the New button, then Apply to create a new valid drive that Windows 10 can be installed on. You'll be asked what additional partitions will be created, click OK to accept. Choose the largest partition size and click Next to install Windows 10.


Windows Setup

Where do you want to install Windows?

Name	Total size	Free space	Type
Drive 0 Partition 1: System Reserved	500.0 MB	483.0 MB	System
Drive 0 Partition 2	31.5 GB	31.5 GB	Primary

Refresh
Delete
Format
New
Load driver
Extend
Next

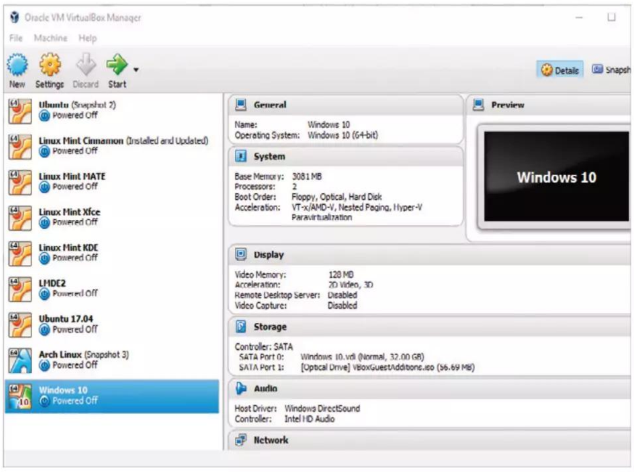
Creating VirtualBox Snapshots of Windows 10

One day the testing process of a Windows 10 VM will inevitably leave the system in a broken or malware riddled state. You can wipe it and start again but a far better solution is to create snapshots, so you can easily revert to a previous build.

Take a Snapshot

Setting up Windows 10, installing the drivers, updates and programs takes a fair amount of time. If you take a VirtualBox snapshot, you can return to where you left off in an instant.

STEP 1 To begin with open VirtualBox. If it's already open, shutdown the Windows 10 VirtualBox image you created. It's not necessary but it's often easier, to ensure the VM is closed prior to creating a snapshot.


Oracle VM VirtualBox Manager
File Machine Help
New Settings Discard Start
Details Snapsh
Ubuntu (Snapshot 2) Powered Off
Linux Mint Cinnamon (Installed and Updated) Powered Off
Linux Mint MATE Powered Off
Linux Mint Xfce Powered Off
Linux Mint KDE Powered Off
LMDE2 Powered Off
Ubuntu 17.04 Powered Off
Arch Linux (Snapshot 3) Powered Off
Windows 10 Powered Off
Preview
Windows 10

General
Name: Windows 10
Operating System: Windows 10 (64-bit)

System
Base Memory: 3081 MB
Processors: 2
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, Hyper-V Paravirtualization

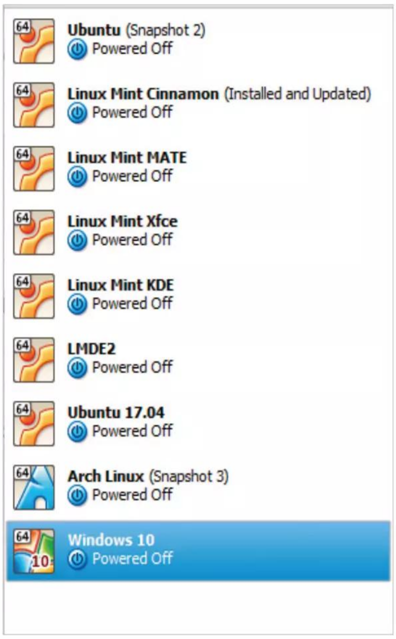
Display
Video Memory: 128 MB
Acceleration: 2D Video, 3D
Remote Desktop Server: Disabled
Video Capture: Disabled

Storage
Controller: SATA
SATA Port 0: Windows 10.vdi (Normal, 32.00 GB)
SATA Port 1: [Optical Drive] VBoxGuestAdditions.iso (56.69 MB)

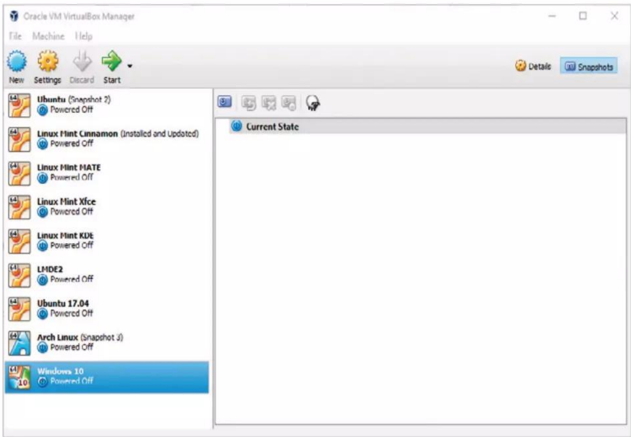
Audio
Host Driver: Windows DirectSound
Controller: Intel HD Audio

Network

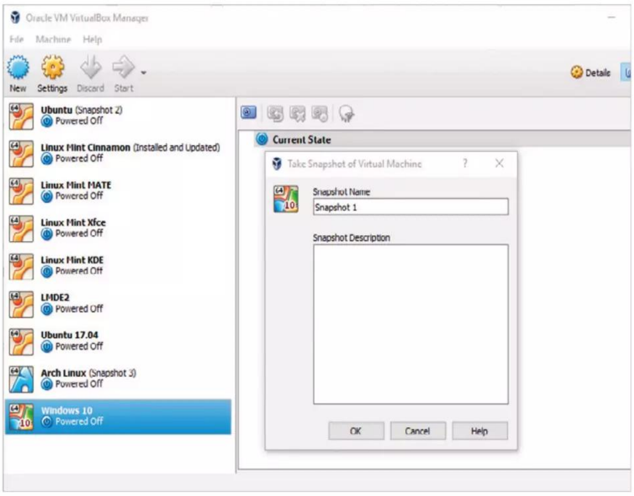
STEP 2 A Snapshot in VirtualBox is simply an image of what the virtual machine 'looked' like at the time the Snapshot was taken. You can make multiple Snapshots and revert to any whenever you wish. Snapshots taken are labelled next to the name of the VM.


Ubuntu (Snapshot 2) Powered Off
Linux Mint Cinnamon (Installed and Updated) Powered Off
Linux Mint MATE Powered Off
Linux Mint Xfce Powered Off
Linux Mint KDE Powered Off
LMDE2 Powered Off
Ubuntu 17.04 Powered Off
Arch Linux (Snapshot 3) Powered Off
Windows 10 Powered Off

STEP 3 You can see that the state of all the virtual systems is currently Powered Off. To create a Snapshot of the Windows 10 VM, click to highlight the system's entry in VirtualBox, then click on the Snapshots button (it's a camera icon), located to the far-right of the VirtualBox console.

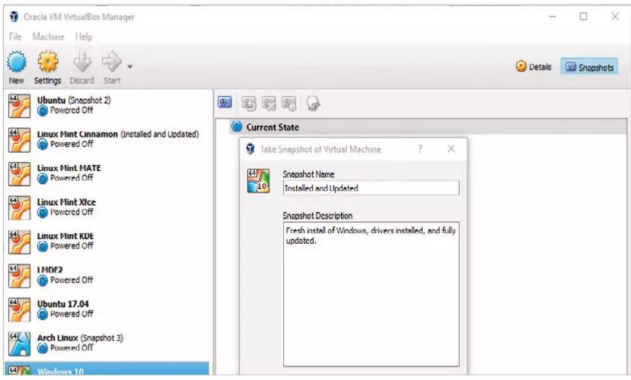

Oracle VM VirtualBox Manager
File Machine Help
New Settings Discard Start
Details Snapshots
Ubuntu (Snapshot 2) Powered Off
Linux Mint Cinnamon (Installed and Updated) Powered Off
Linux Mint MATE Powered Off
Linux Mint Xfce Powered Off
Linux Mint KDE Powered Off
LMDE2 Powered Off
Ubuntu 17.04 Powered Off
Arch Linux (Snapshot 3) Powered Off
Windows 10 Powered Off
Current State

STEP 4 At present there aren't any Snapshots of Windows 10 available. To create one, click the camera icon just above the words Current State, the icon at the opposite end of the sheep icon. This will launch the Take Snapshot of Virtual Machine console window.


Oracle VM VirtualBox Manager
File Machine Help
New Settings Discard Start
Details
Ubuntu (Snapshot 2) Powered Off
Linux Mint Cinnamon (Installed and Updated) Powered Off
Linux Mint MATE Powered Off
Linux Mint Xfce Powered Off
Linux Mint KDE Powered Off
LMDE2 Powered Off
Ubuntu 17.04 Powered Off
Arch Linux (Snapshot 3) Powered Off
Windows 10 Powered Off
Current State
Take Snapshot of Virtual Machine
Snapshot Description
OK
Cancel
Help

Snapshot Name: Snapshot 1

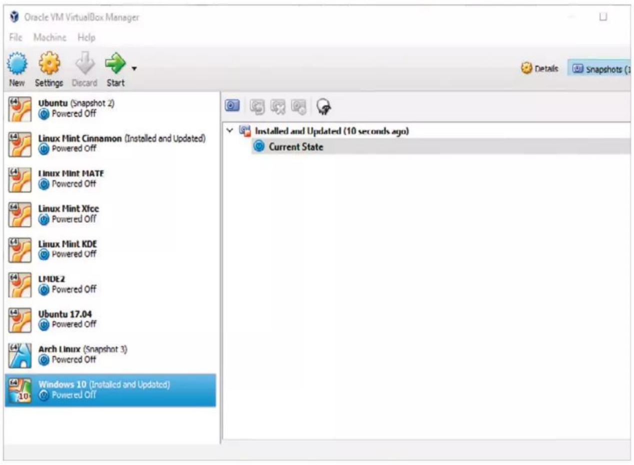
STEP 5 If you want you can name the Snapshot: Installed and Updated for example, along with a description to help identify it easier from the other Snapshots you may eventually end up making. It's not hugely important but if someone else wants to load up Windows 10, they know which Snapshot to go for. When you're done, click the OK button.


Oracle VM VirtualBox Manager
File Machine Help
New Settings Discard Start
Details Snapshots
Ubuntu (Snapshot 2) Powered Off
Linux Mint Cinnamon (Installed and Updated) Powered Off
Linux Mint MATE Powered Off
Linux Mint Xfce Powered Off
Linux Mint KDE Powered Off
LMDE2 Powered Off
Ubuntu 17.04 Powered Off
Arch Linux (Snapshot 3) Powered Off
Windows 10
Current State
Take Snapshot of Virtual Machine

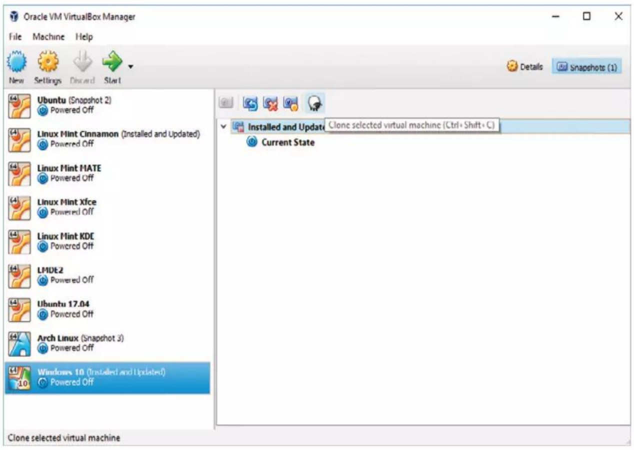
Snapshot Name: Installed and Updated

Snapshot Description: Fresh install of Windows, drivers installed, and fully updated.

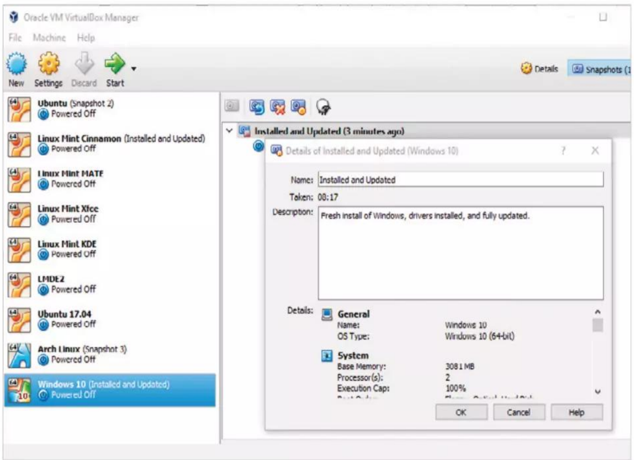
STEP 6 The process happens almost instantly and you're left with an entry in the Snapshots section detailing the named Snapshot, how long ago it was taken and a Current State entry. The Current State is literally its state when you boot it up. With it highlighted, you can take more Snapshots by using the camera icon again.


Oracle VM VirtualBox Manager
File Machine Help
New Settings Discard Start
Details Snapshots (1)
Ubuntu (Snapshot 2) Powered Off
Linux Mint Cinnamon (Installed and Updated) Powered Off
Linux Mint MATE Powered Off
Linux Mint Xfce Powered Off
Linux Mint KDE Powered Off
LMDE2 Powered Off
Ubuntu 17.04 Powered Off
Arch Linux (Snapshot 3) Powered Off
Windows 10 (Installed and Updated) Powered Off
Installed and Updated (10 seconds ago)
Current State

STEP 7 If you click the named Snapshot, you get more options available in the toolbar just above. Here you can Restore a selected Snapshot, if you have multiple entries. You can Delete a Snapshot and view detailed information regarding one; and with the sheep, you can Clone the current Snapshot as a new virtual machine.


Oracle VM VirtualBox Manager
File Machine Help
New Settings Discard Start
Details Snapshots (1)
Ubuntu (Snapshot 2) Powered Off
Linux Mint Cinnamon (Installed and Updated) Powered Off
Linux Mint MATE Powered Off
Linux Mint Xfce Powered Off
Linux Mint KDE Powered Off
LMDE2 Powered Off
Ubuntu 17.04 Powered Off
Arch Linux (Snapshot 3) Powered Off
Windows 10 (Installed and Updated) Powered Off
Installed and Updat
Clone selected virtual machine (Ctrl+Shift+C)
Current State
Clone selected virtual machine

STEP 8 If you click the Details of the named virtual machine icon, the one next to the sheep, represented with an orange circle, you can view the VirtualBox settings of that particular Snapshot. This way you can assess any issues that may arise with other virtual machines; here you can see which settings worked and which didn't.


Oracle VM VirtualBox Manager
File Machine Help
New Settings Discard Start
Details Snapshots (1
Ubuntu (Snapshot 2) Powered Off
Linux Mint Cinnamon (Installed and Updated) Powered Off
Linux Mint MATE Powered Off
Linux Mint Xfce Powered Off
Linux Mint KDE Powered Off
LMDE2 Powered Off
Ubuntu 17.04 Powered Off
Arch Linux (Snapshot 3) Powered Off
Windows 10 (Installed and Updated) Powered Off
Installed and Updated (3 minutes ago)
Details of Installed and Updated (Windows 10)
OK
Cancel
Help

Name: Installed and Updated

Taken: 08:17

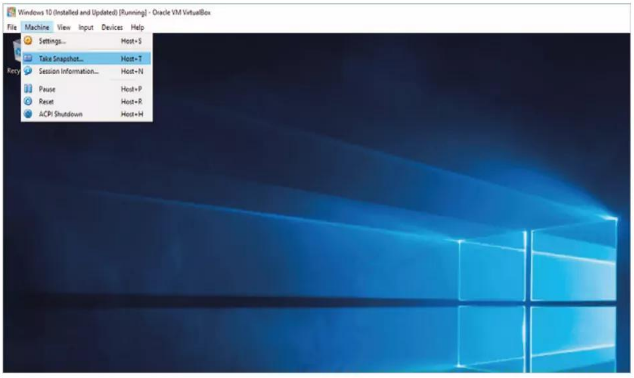
Description: Fresh install of Windows, drivers installed, and fully updated.

Details:

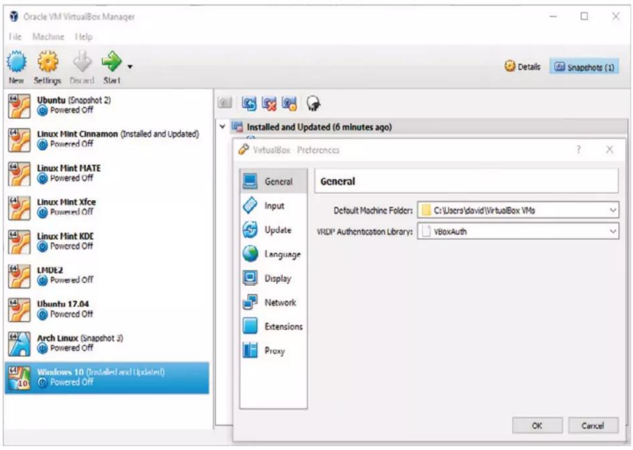
General
Name: Windows 10
OS Type: Windows 10 (64-bit)

System
Base Memory: 3081 MB
Processor(s): 2
Execution Cap: 100%

STEP 9 You shutdown the guest system, as mentioned in Step 1, but VirtualBox guest doesn't need to be shutdown in order for a Snapshot to be taken. For example, prior to installing an experimental program, click the Machine entry in the VirtualBox top menu bar and choose Take Snapshot. The process works the same way as in Steps 4 onward.


Windows 10 (Installed and Updated) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Settings... Host+S
Take Snapshot... Host+T
Session Information... Host+N
Pause Host+P
Reset Host+R
ACPI Shutdown Host+H

STEP 10 Each Snapshot taken can easily be reverted to, cloned, deleted and so on. However, Snapshots are stored by default in the Users/username/VirtualBox VMs folder in Windows. If you've only a limited amount of space on your C:\ drive, you may want to set the path to a bigger hard drive in the File > Preferences option in VirtualBox.


Oracle VM VirtualBox Manager
File Machine Help
New Settings Discard Start
Details Snapshots (1)
Ubuntu (Snapshot 2) Powered Off
Linux Mint Cinnamon (Installed and Updated) Powered Off
Linux Mint MATE Powered Off
Linux Mint Xfce Powered Off
Linux Mint KDE Powered Off
LMDE2 Powered Off
Ubuntu 17.04 Powered Off
Arch Linux (Snapshot 3) Powered Off
Windows 10 (Installed and Updated) Powered Off
Installed and Updated (6 minutes ago)
VirtualBox - Preferences
General
Input
Update
Language
Display
Network
Extensions
Proxy
OK
Cancel

General

Default Machine Folder: C:\Users\david\VirtualBox VMs

VRDP Authentication Library: VBoxAuth

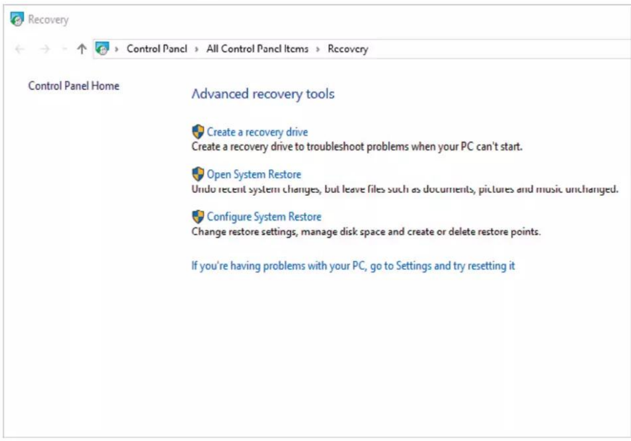
Create a Windows 10 Recovery Drive

Since Windows 95, Microsoft has offered users the ability to create a recovery drive, which is used to help troubleshoot a Windows PC that is failing to boot, by presenting various options. If you haven't done so yet, you ideally should have created a Windows 10 recovery drive.

Time to Recover

You need an 8GB USB drive minimum, in order to successfully create a recovery drive. It wipes the contents off the drive and you won't be able to use it for anything else, so make sure it's labelled and stored in a safe place.

STEP 1 Insert the USB drive into your PC and close the Explorer window that opens upon insertion. Click the Windows Start button and type recovery, then click on the Recovery Control Panel. In here you can see several options available; you want the first, Create a recovery drive.



Recovery

Control Panel › All Control Panel Items › Recovery

Control Panel Home

Advanced recovery tools

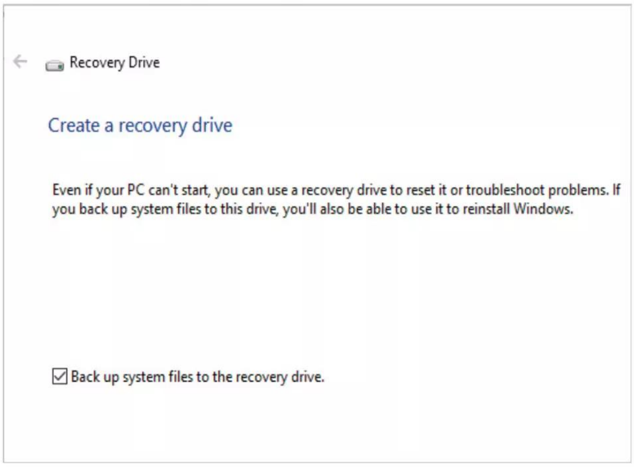
Create a recovery drive
Create a recovery drive to troubleshoot problems when your PC can't start.

Open System Restore
Undo recent system changes, but leave files such as documents, pictures and music unchanged.

Configure System Restore
Change restore settings, manage disk space and create or delete restore points.

If you're having problems with your PC, go to Settings and try resetting it

STEP 2 Click the Create a recovery drive link and accept the UAC authentication message that pops up. First, there's the option to backup any important system files to the recovery drive, alongside the usual recovery options. This is a good idea as it can replace these vital files in the event of a boot failure. Click Next to continue.



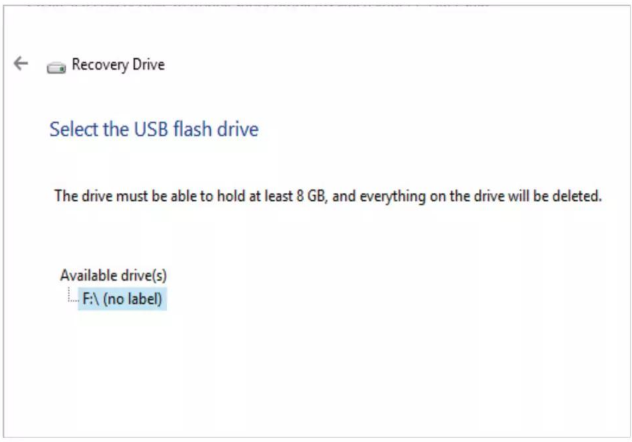
Recovery Drive

Create a recovery drive

Even if your PC can't start, you can use a recovery drive to reset it or troubleshoot problems. If you back up system files to this drive, you'll also be able to use it to reinstall Windows.

☑ Back up system files to the recovery drive.

STEP 3 There's a short wait as Windows analyses the available locations where it can install and create the recovery drive. Eventually, providing you inserted the 8GB plus USB stick prior to starting the process, you're asked to select the destination from those Windows has discovered.



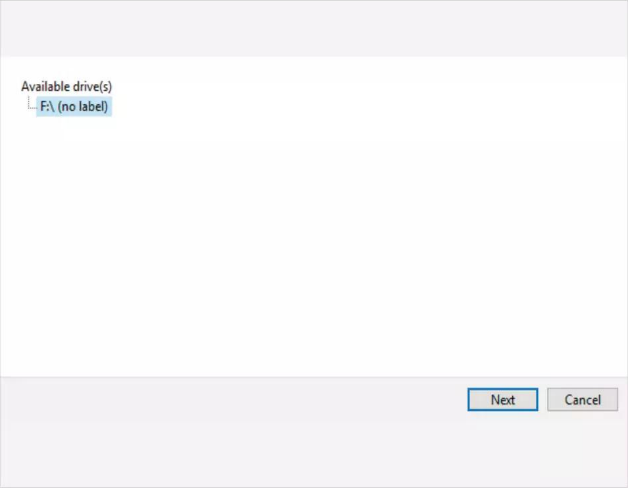
Recovery Drive

Select the USB flash drive

The drive must be able to hold at least 8 GB, and everything on the drive will be deleted.

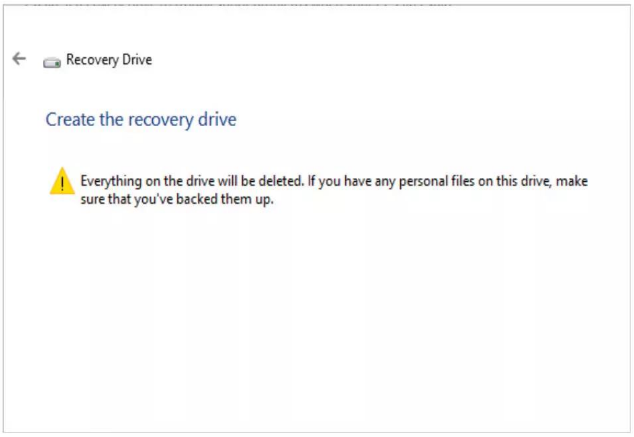
Available drive(s)
F:\ (no label)

STEP 4 In the example we have here, there's just one possible location, the F:\ drive. If you have more than one possible destination available, make sure that you're selecting the correct USB drive for your recovery drive. When you're ready, click on the Next button.



Available drive(s)
F:\ (no label)

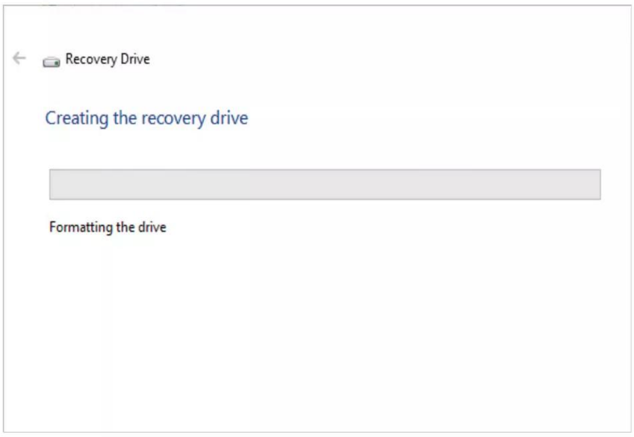
STEP 5 Before committing to creating the recovery drive, Windows will offer one final warning. Remember, everything that's currently on the USB stick you chose as the recovery drive will be erased during the process of creating the drive. If you have any files stored on it, make sure they're backed up to another location.


Recovery Drive

Create the recovery drive

Everything on the drive will be deleted. If you have any personal files on this drive, make sure that you've backed them up.

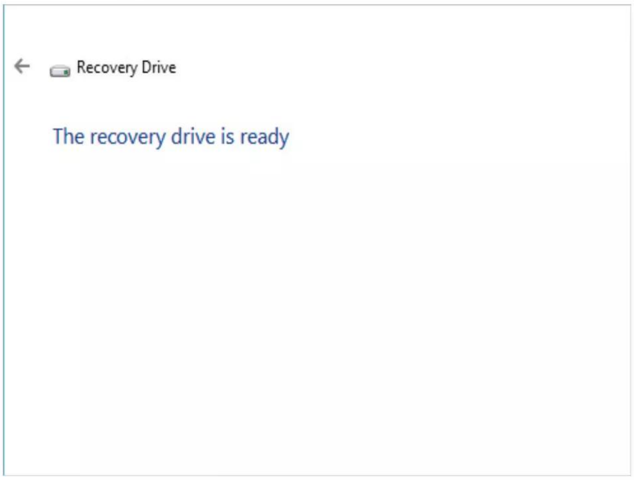
STEP 6 When you're ready click on the Create button to start the process. It may take some time, depending on the speed of the USB stick used, as Windows prepares, formats and copies the utilities and files over to the USB recovery drive.


Recovery Drive

Creating the recovery drive

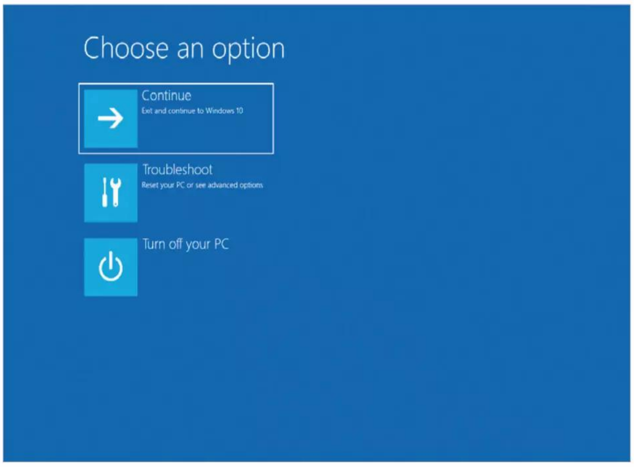
Formatting the drive

STEP 7 When the process is complete, you receive a recovery drive is ready message. The only option available to you is to click the Finish button. This will close the recovery drive window and return you to the Recovery console.


Recovery Drive

The recovery drive is ready

STEP 8 Store the drive in a safe place, as it can restore vital system files should anything ever go wrong with your system and leave it unable to boot. Should something go wrong, you see the Windows 10 safe mode boot options when you try and power up your computer.

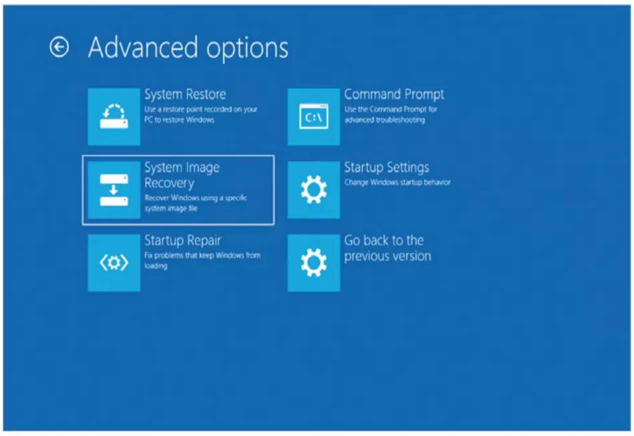

Choose an option

Continue
Exit and continue to Windows 10

Troubleshoot
Reset your PC or see advanced options

Turn off your PC

STEP 9 From the safe mode boot options, choose the Troubleshoot tile followed by Advanced Options. From there you can choose the System Restore and System Image Recovery options along with your rescue drive to help you recover Windows.


Advanced options

System Restore
Use a restore point recorded on your PC to restore Windows

Command Prompt
Use the Command Prompt for advanced troubleshooting

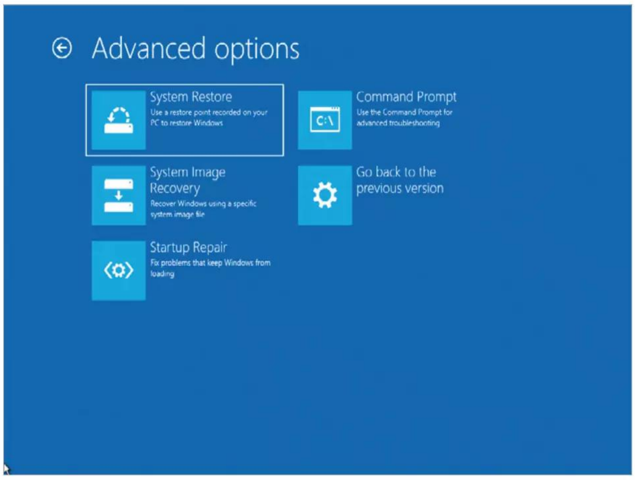
System Image Recovery
Recover Windows using a specific system image file

Startup Settings
Change Windows startup behavior

Startup Repair
Fix problems that keep Windows from loading

Go back to the previous version

STEP 10 Alternatively, set the BIOS to boot to the newly created recovery drive and follow the onscreen instructions to launch the recovery method. Start by choosing your language, then select the Troubleshoot option and then opt for one of several recovery options.


Advanced options

System Restore
Use a restore point recorded on your PC to restore Windows

Command Prompt
Use the Command Prompt for advanced troubleshooting

System Image Recovery
Recover Windows using a specific system image file

Go back to the previous version

Startup Repair
Fix problems that keep Windows from loading

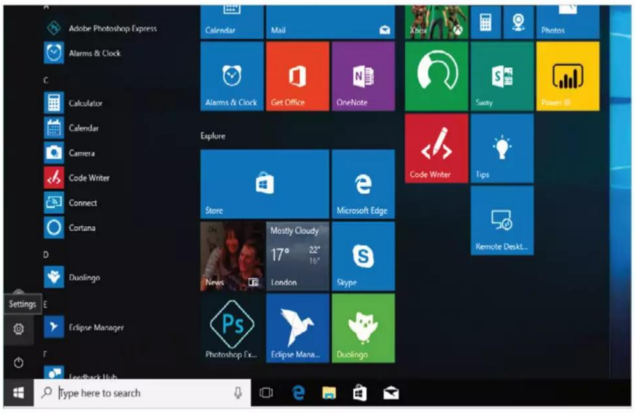
How to Back Up Windows 10

Even with the greatest possible cyber protection in the world guarding your computer, there's still a chance something could go wrong. It might not even be malware-related; a broken hard drive or other component can cause as much grief. Therefore, you need a good backup.

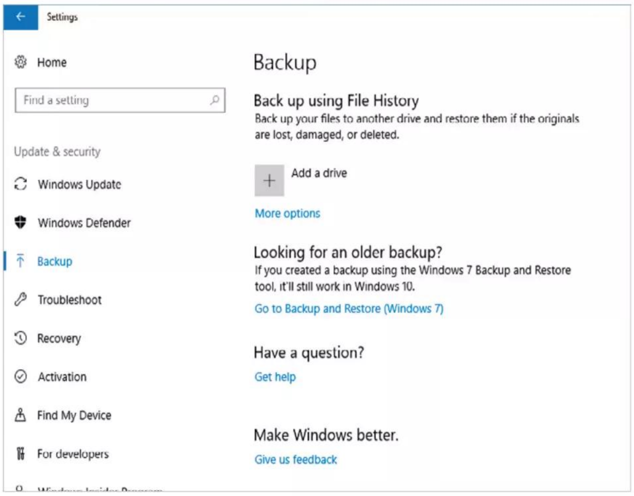
Backing Up

Computers are unpredictable beasts, so you need to make sure that all your files and important data are securely backed up and more importantly, you're able to restore them easily. Thankfully, it's a straightforward process.

STEP 1 Windows has, since its early days, featured some form of backup tool. Windows 10 was launched with the File History backup tool, which is a simple to use tool to ensure stable and regular backups of important files are made. Start by clicking on the Windows Start button and selecting Settings from the menu.


Adobe Photoshop Express
Alarms & Clock
C
Calculator
Calendar
Camera
Code Writer
Connect
Cortana
D
Duolingo
Settings
E
Eclipse Manager
F
Feedback Hub
Type here to search
Calendar
Mail
Xbox
Photos
Alarms & Clock
Get Office
OneNote
Sway
Power BI
Explore
Code Writer
Tips
Store
Microsoft Edge
Remote Deskt...
Mostly Cloudy
17°
22°
15°
News
London
Skype
Photoshop Ex...
Eclipse Mana...
Duolingo

STEP 2 Once in the Settings console, click on the Update & Security icon, followed by the Backup option from the menu on the left. You can see a number of possible options before you: Add a Drive, More options, Go to Backup and Restore (Windows 7), along with help and feedback links.


Settings
Home
Find a setting
Update & security
Windows Update
Windows Defender
Backup
Troubleshoot
Recovery
Activation
Find My Device
For developers

Backup

Back up using File History

Back up your files to another drive and restore them if the originals are lost, damaged, or deleted.

+ Add a drive

More options

Looking for an older backup?

If you created a backup using the Windows 7 Backup and Restore tool, it'll still work in Windows 10.

Go to Backup and Restore (Windows 7)

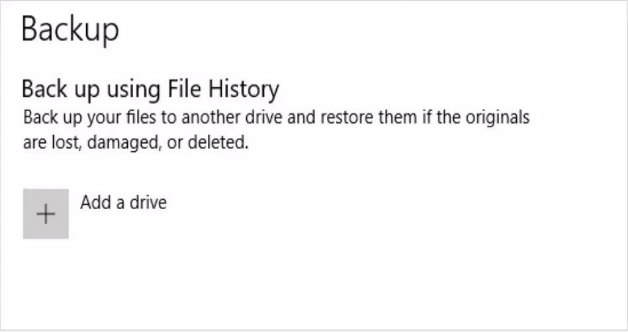
Have a question?

Get help

Make Windows better.

Give us feedback

STEP 3 Ideally you need to insert a reasonably sized USB stick or use a second hard drive in your computer. If you have a USB stick, insert it now, or if you own a second hard drive power off the computer and install it and boot back into Windows 10. Once done, click the Add a Drive icon.



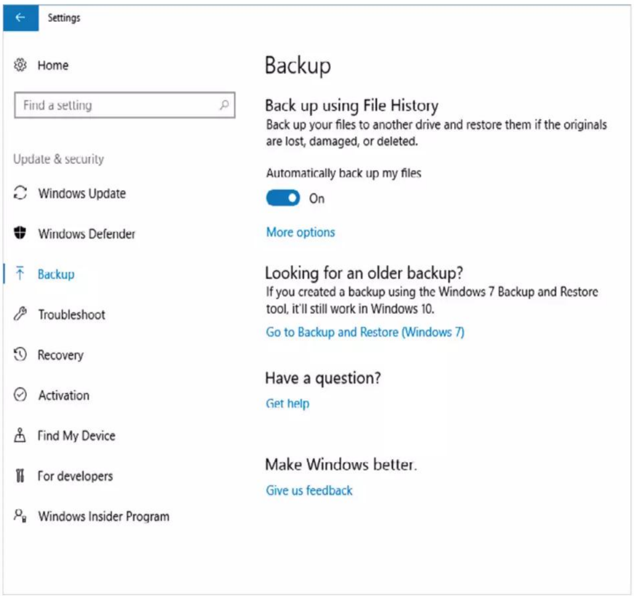
Backup

Back up using File History

Back up your files to another drive and restore them if the originals are lost, damaged, or deleted.

+ Add a drive

STEP 4 Windows will search for any capable drives on to which it's able to back up your files. When your drive or USB device is displayed, click the drive link. Notice that an 'Automatically back up my files' switch button has appeared where Add a drive once was.


Settings
Home
Find a setting
Update & security
Windows Update
Windows Defender
Backup
Troubleshoot
Recovery
Activation
Find My Device
For developers
Windows Insider Program

Backup

Back up using File History

Back up your files to another drive and restore them if the originals are lost, damaged, or deleted.

Automatically back up my files

● On

More options

Looking for an older backup?

If you created a backup using the Windows 7 Backup and Restore tool, it'll still work in Windows 10.

Go to Backup and Restore (Windows 7)

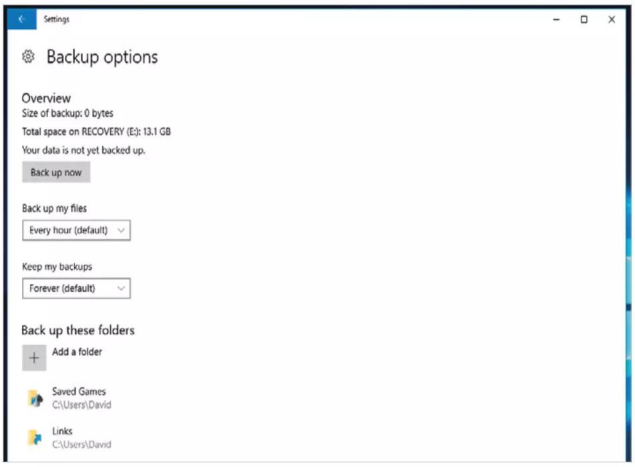
Have a question?

Get help

Make Windows better.

Give us feedback

STEP 5 From here, click on the More Options link that's under the switch button, this will open the Backup Options console. This section details the backup schedule, the location and which folders will be included in the backup; and for how long Windows will retain your backed up files.


Settings

Backup options

Overview
Size of backup: 0 bytes
Total space on RECOVERY (E:): 13.1 GB
Your data is not yet backed up.

Back up now

Back up my files: Every hour (default)

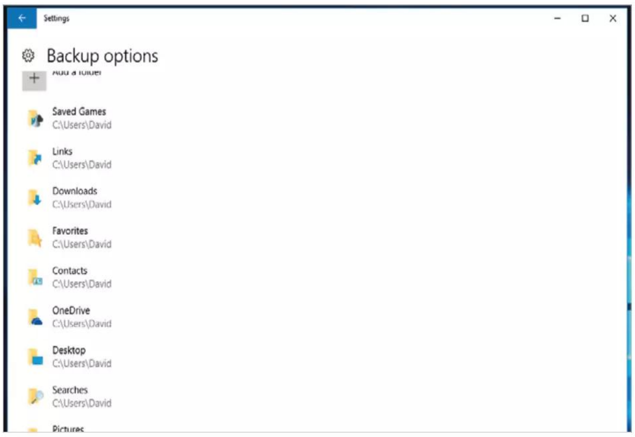
Keep my backups: Forever (default)

Back up these folders

Add a folder

Saved Games
C:\Users\David
Links
C:\Users\David

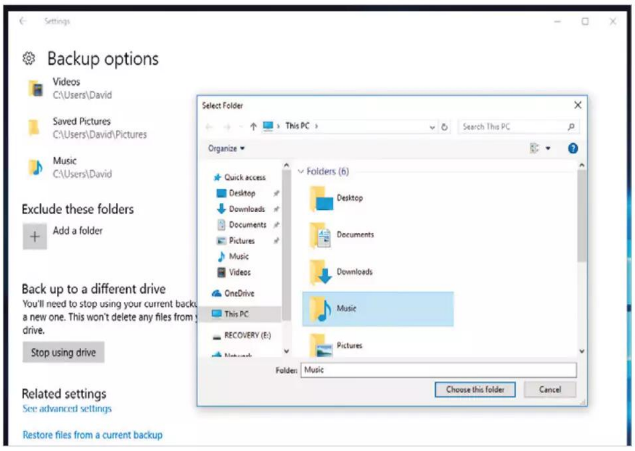
STEP 6 If you scroll down through the Backup Options console, you can see that the entirety of your user folder within Windows 10 has been added by default. This includes the Music and Videos folders, as well as Searches, Camera Roll, Contacts, Favourites and so on.


Settings

Backup options

Saved Games
C:\Users\David
Links
C:\Users\David
Downloads
C:\Users\David
Favorites
C:\Users\David
Contacts
C:\Users\David
OneDrive
C:\Users\David
Desktop
C:\Users\David
Searches
C:\Users\David
Pictures

STEP 7 At the bottom of the console window you have the options to stop using the selected drive and to Exclude any folders from the default. If you don't want to back up folders for Music, Videos etc., click Add a folder on the Exclude these folders icon, then pick the folder to exclude and click the Choose this folder button.


Settings

Backup options

Videos
C:\Users\David
Saved Pictures
C:\Users\David\Pictures
Music
C:\Users\David

Exclude these folders

Add a folder

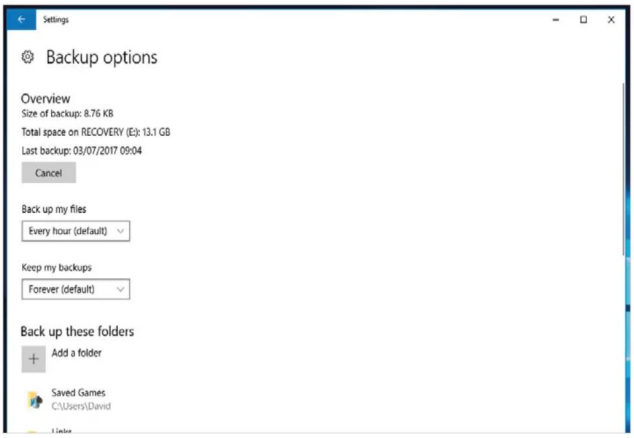
Back up to a different drive
You'll need to stop using your current backu
a new one. This won't delete any files from y
drive.

Stop using drive
Related settings
See advanced settings
Restore files from a current backup
Select Folder
This PC
Search This PC
Organize
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
RECOVERY (E:)
Folders (6)
Desktop
Documents
Downloads
Music
Pictures

Folder: Music

Choose this folder
Cancel

STEP 8 When you're ready to start backing up, you can click the Back up now button to the top of the Backup Option console window. Alternatively, you can wait for an hour when the default schedule kicks in. Obviously, depending on the size of the files within your backup folders this could take some time.


Settings

Backup options

Overview
Size of backup: 8.76 KB
Total space on RECOVERY (E:): 13.1 GB
Last backup: 03/07/2017 09:04

Cancel

Back up my files: Every hour (default)

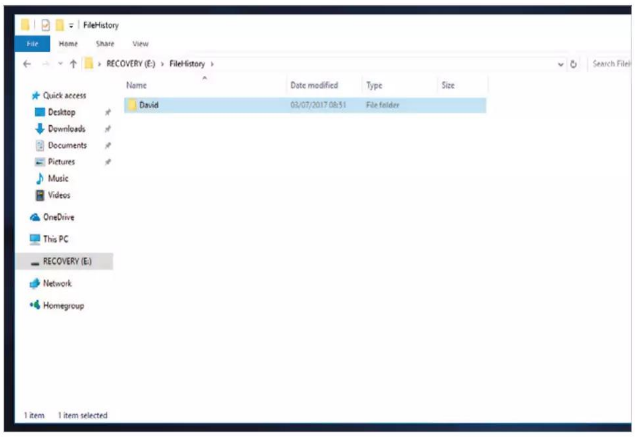
Keep my backups: Forever (default)

Back up these folders

Add a folder

Saved Games
C:\Users\David

STEP 9 The backed up files will be stored on the chosen backup drive, within a folder called FileHistory. Inside that folder will be the specific user folder, so if you use File History backups for more than one user, their user names will be listed here too.


FileHistory

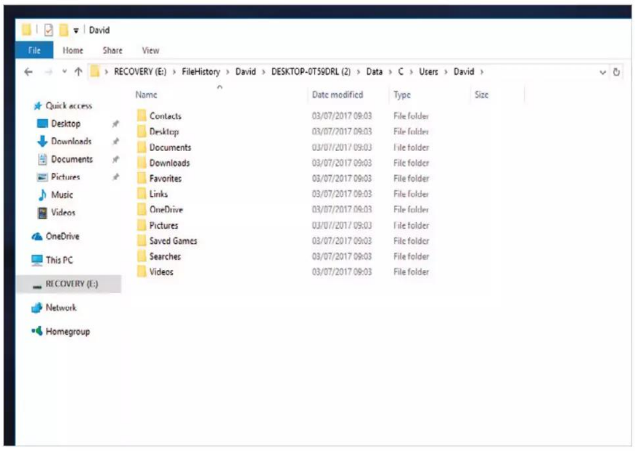
RECOVERY (E:) › FileHistory ›

Name	Date modified	Type	Size
David	03/07/2017 08:51	File folder	

1 item 1 item selected

File
Home
Share
View
Search File
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
RECOVERY (E:)
Network
Homegroup

STEP 10 Drilling deeper into the folder layers reveals more default folders, containing important XML data that Windows uses to store the chosen options. You can find the actual files that have been backed up in the Data folder, laid out in the same folder structure as on your system, i.e. C > Users > Name > Documents etc.


David

RECOVERY (E:) › FileHistory › David › DESKTOP-0T59DRL (2) › Data › C › Users › David ›

Name	Date modified	Type	Size
Contacts	03/07/2017 09:03	File folder	
Desktop	03/07/2017 09:03	File folder	
Documents	03/07/2017 09:03	File folder	
Downloads	03/07/2017 09:03	File folder	
Favorites	03/07/2017 09:03	File folder	
Links	03/07/2017 09:03	File folder	
OneDrive	03/07/2017 09:03	File folder	
Pictures	03/07/2017 09:03	File folder	
Saved Games	03/07/2017 09:03	File folder	
Searches	03/07/2017 09:03	File folder	
Videos	03/07/2017 09:03	File folder	

File
Home
Share
View
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
RECOVERY (E:)
Network
Homegroup

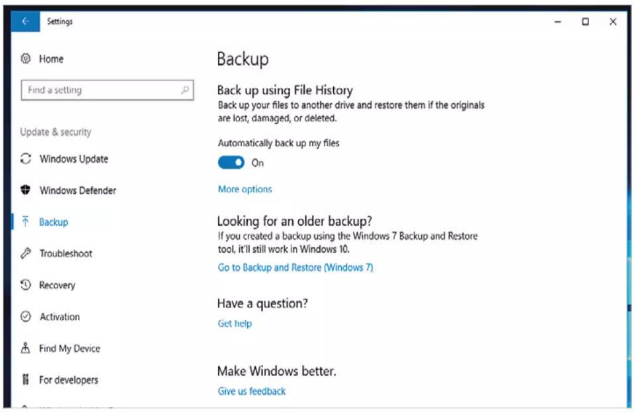
How to Create a Windows 10 System Image

Backing up your files is perfectly fine but in the event of having to wipe your hard drive and start again, getting everything back in order can be time consuming. However, creating a system image means you can almost instantly restore the entire system without needing to rebuild Windows.

System Imaging

A system image works in much the same way as the VirtualBox Snapshots. You're essentially taking a snapshot of your entire system, which can then be restored quickly. Saving you having to reinstall Windows 10, all your programs and data.

STEP 1 To begin, click on the Windows Start button and once more navigate to Settings > Update & Security > Backup. From within the Backup console window, where you were in the previous tutorial, click on the Go to Backup and Restore (Windows 7) link under the Looking for an older backup section.


Settings
Home
Find a setting
Update & security
Windows Update
Windows Defender
Backup
Troubleshoot
Recovery
Activation
Find My Device
For developers

Backup

Back up using File History

Back up your files to another drive and restore them if the originals are lost, damaged, or deleted.

Automatically back up my files: On

More options

Looking for an older backup?

If you created a backup using the Windows 7 Backup and Restore tool, it'll still work in Windows 10.

Go to Backup and Restore (Windows 7)

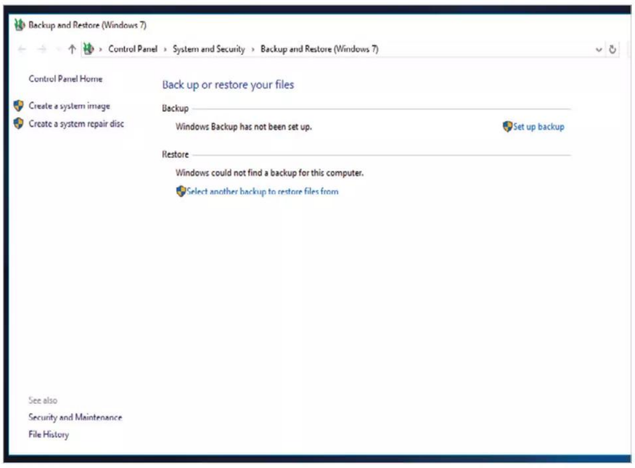
Have a question?

Get help

Make Windows better.

Give us feedback

STEP 2 This will launch a new window, the Backup and Restore (Windows 7) console. Microsoft has kept this feature intact through Windows 8.1 and 10 purely due to compatibility support for backups done under older versions of the OS. To the left there are two links, click on the Create a system image link.


Backup and Restore (Windows 7)
Control Panel › System and Security › Backup and Restore (Windows 7)
Control Panel Home
Create a system image
Create a system repair disc
See also
Security and Maintenance
File History

Back up or restore your files

Backup

Windows Backup has not been set up.

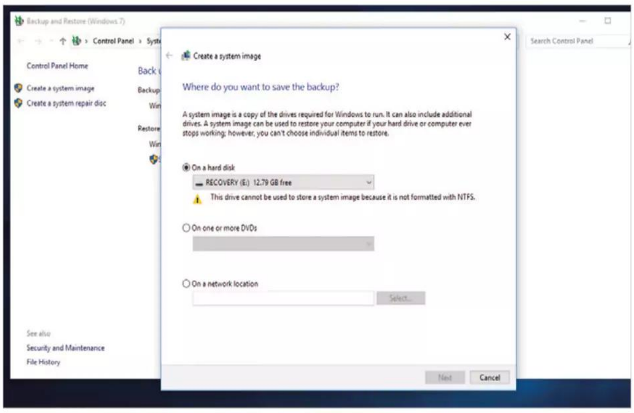
Set up backup

Restore

Windows could not find a backup for this computer.

Select another backup to restore files from

STEP 3 Windows will now scan your system for a drive that is able to house the system image files. You may need to make some changes to any drives according to what messages you get back from the scan. In this example, the drive we're using needs to be formatted as NTFS before Windows 10 can use it.


Backup and Restore (Windows 7)
Control Panel
Search Control Panel
Control Panel Home
Create a system image
Create a system repair disc
See also
Security and Maintenance
File History
Create a system image
Select...
Next
Cancel

Where do you want to save the backup?

A system image is a copy of the drives required for Windows to run. It can also include additional drives. A system image can be used to restore your computer if your hard drive or computer ever stops working; however, you can't choose individual items to restore.

● On a hard disk

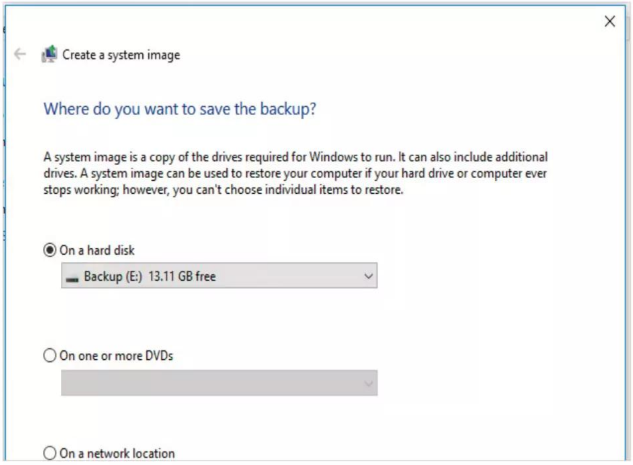
RECOVERY (E:) 12.79 GB free

This drive cannot be used to store a system image because it is not formatted with NTFS.

○ On one or more DVDs

○ On a network location

STEP 4 Providing you've met the requirements, you're offered a choice of where the system image can be written to. A drive is the quickest solution when it comes to restoring the image but you can opt for DVDs; it depends on the size of the image as to how many DVDs you need. You can even select a network location.


Create a system image

Where do you want to save the backup?

A system image is a copy of the drives required for Windows to run. It can also include additional drives. A system image can be used to restore your computer if your hard drive or computer ever stops working; however, you can't choose individual items to restore.

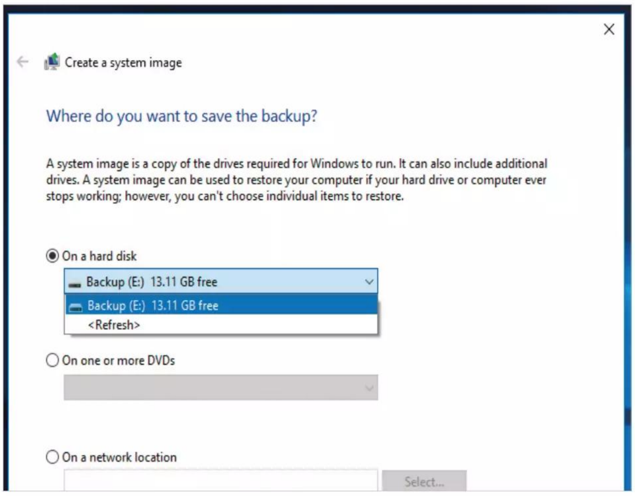
● On a hard disk

Backup (E:) 13.11 GB free

○ On one or more DVDs

○ On a network location

STEP 5 For this example, let's use an internal second hard drive. Make sure that the correct drive (it could be a high capacity USB stick or even portable USB hard drive) is selected, then click the Next button to continue.



Where do you want to save the backup?

A system image is a copy of the drives required for Windows to run. It can also include additional drives. A system image can be used to restore your computer if your hard drive or computer ever stops working; however, you can't choose individual items to restore.

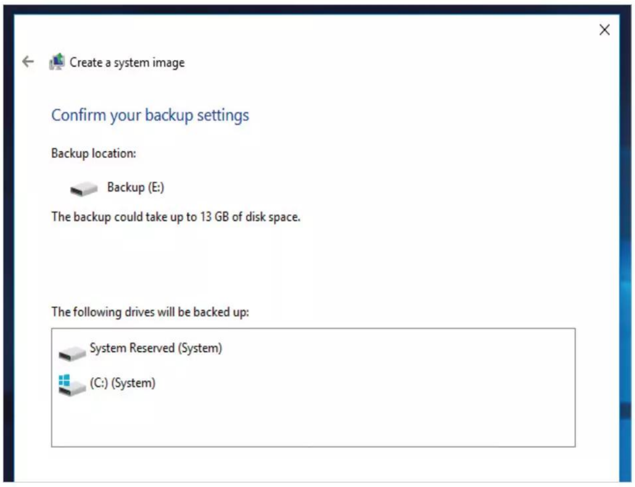
● On a hard disk

Backup (E:) 13.11 GB free

○ On one or more DVDs

○ On a network location

STEP 6 The next window will display the drives that are included in the system imaging process. In this example, the C:\ drive, the system drive and the System Reserved partition are to be backed up. When it comes to restoring the system you'll need both partitions for Windows 10 to be able to boot up correctly.



Confirm your backup settings

Backup location:

Backup (E:)

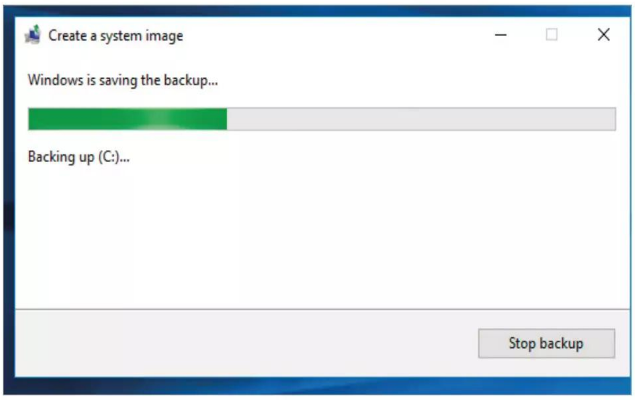
The backup could take up to 13 GB of disk space.

The following drives will be backed up:

System Reserved (System)

(C:) (System)

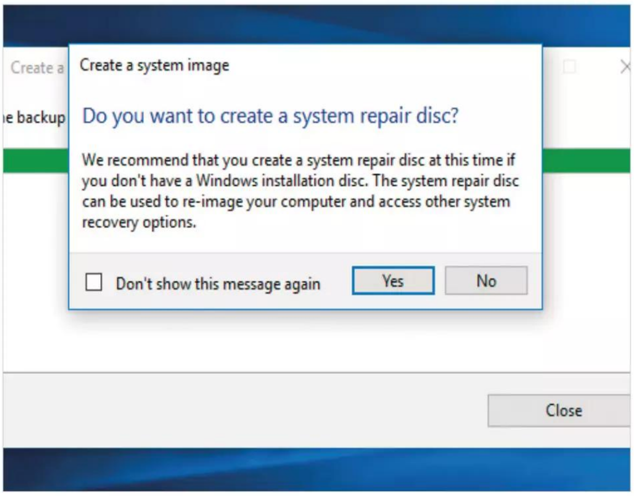
STEP 7 When you're ready to continue, click the Start Backup button. This will begin the imaging process, which can take some time depending on the amount of space used on the C:\ drive and the speed of the drive you're writing to. Allocate ample time if you're writing to DVD.



Windows is saving the backup...

Backing up (C:)...

STEP 8 Once the process is complete, Windows will ask you to create a System Repair Disc. This disc will allow you to boot into the environment where you are able to launch the system image restore.

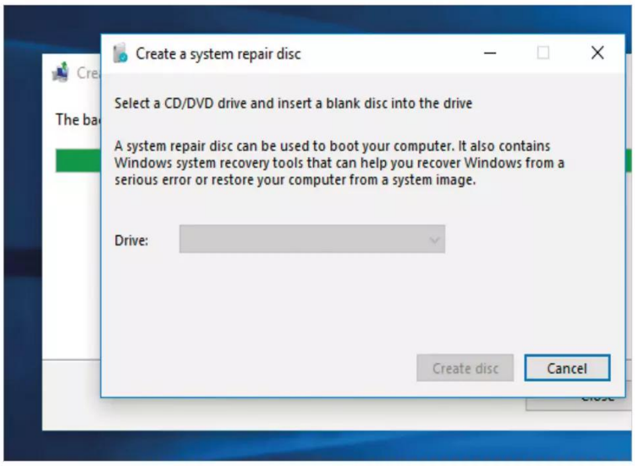


Do you want to create a system repair disc?

We recommend that you create a system repair disc at this time if you don't have a Windows installation disc. The system repair disc can be used to re-image your computer and access other system recovery options.

☐ Don't show this message again

STEP 9 If you click Yes to creating the System Repair Disc you need to make sure you have a blank DVD to hand. Follow the on-screen instructions and click on the Create Disc button to burn the repair files to the disc.

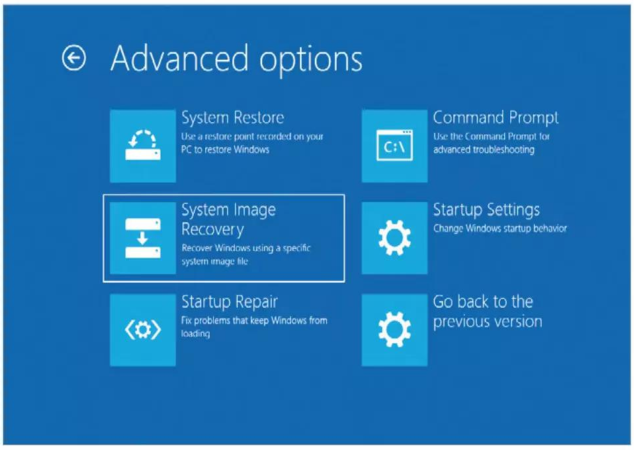


Select a CD/DVD drive and insert a blank disc into the drive

A system repair disc can be used to boot your computer. It also contains Windows system recovery tools that can help you recover Windows from a serious error or restore your computer from a system image.

Drive:

STEP 10 Should you need to restore Windows 10 from the system image, you can boot into the System Repair Disc and select the System Image Recovery option from within the Advanced Options of the Trouble Shoot menu. Follow the instructions and within minutes Windows 10 will be back as it was when the system image was taken.


Advanced options

System Restore — Use a restore point recorded on your PC to restore Windows

Command Prompt — Use the Command Prompt for advanced troubleshooting

System Image Recovery — Recover Windows using a specific system image file

Startup Settings — Change Windows startup behavior

Startup Repair — Fix problems that keep Windows from loading

Go back to the previous version

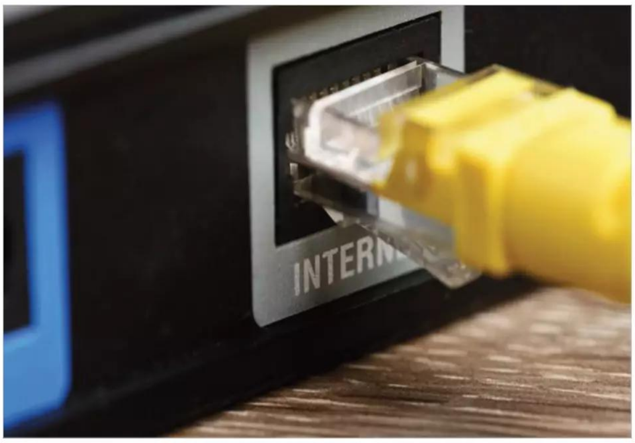
Extreme Windows 10 Lockdown Tips

There are numerous ways and means to greatly improve Windows 10's security and privacy. Precisely how secure and private you want to get is purely down to you. You can opt for better than average or through these tips below, absolute extreme security.

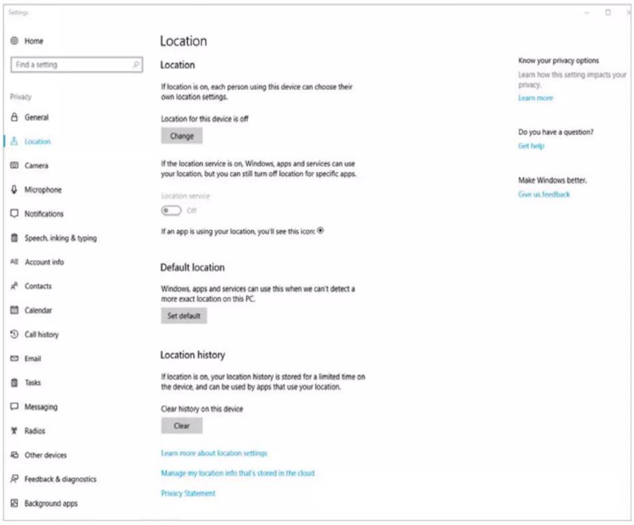
Windows 10 Security: The Paranoid's Guide

If you're fanatical about securing Windows 10 and locking it down to the point where the NSA would be impressed, then follow these top ten extreme lockdown tips.

TIP 1 Let's begin with the easiest tip, unplug the computer from the Internet. Naturally there are disadvantages to this and you won't get updates for Windows or programs. However, you certainly won't get any Internet-borne malware infecting your machine.



TIP 2 Click the Windows Start button and type privacy into the search box. Open the Privacy Settings link and turn off every option within the eighteen available Privacy sub-categories to the left of the console window.


Settings
Home
Find a setting
Privacy
General
Location
Camera
Microphone
Notifications
Speech, inking & typing
Account info
Contacts
Calendar
Call history
Email
Tasks
Messaging
Radios
Other devices
Feedback & diagnostics
Background apps

Location

Location

If location is on, each person using this device can choose their own location settings.

Location for this device is off

Change

If the location service is on, Windows, apps and services can use your location, but you can still turn off location for specific apps.

Location service

Off

If an app is using your location, you'll see this icon: ◉

Default location

Windows, apps and services can use this when we can't detect a more exact location on this PC.

Set default

Location history

If location is on, your location history is stored for a limited time on the device, and can be used by apps that use your location.

Clear history on this device

Clear

Learn more about location settings

Manage my location info that's stored in the cloud

Privacy Statement

Know your privacy options

Learn how this setting impacts your privacy.

Learn more

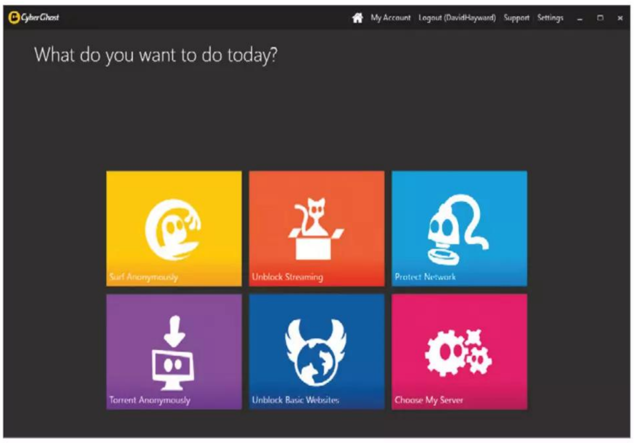
Do you have a question?

Get help

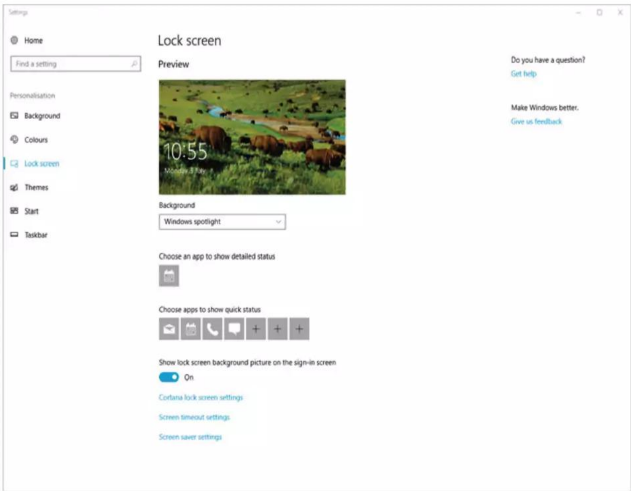
Make Windows better.

Give us feedback

TIP 3 When online use a VPN and where possible, also use the Tor browser. Both of these combined will greatly improve your anonymity and improve security by utilising the site blocking and anti-scamming properties of a good VPN such as CyberGhost.


CyberGhost
My Account
Logout (DavidHayward)
Support
Settings
What do you want to do today?
Surf Anonymously
Unblock Streaming
Protect Network
Torrent Anonymously
Unblock Basic Websites
Choose My Server

TIP 4 If you step away from your computer on regular intervals, you need to make sure that no one will be able to get on to it. From the Windows Start button type lock and click the Lock Screen Settings link. In here set a lock so that only you can get back to your desktop once you've entered a password.


Settings
Home
Find a setting
Personalisation
Background
Colours
Lock screen
Themes
Start
Taskbar
10:55
Monday 3 July

Lock screen

Preview

Background

Windows spotlight

Choose an app to show detailed status

Choose apps to show quick status

Show lock screen background picture on the sign-in screen

On

Cortana lock screen settings

Screen timeout settings

Screen saver settings

Do you have a question?

Get help

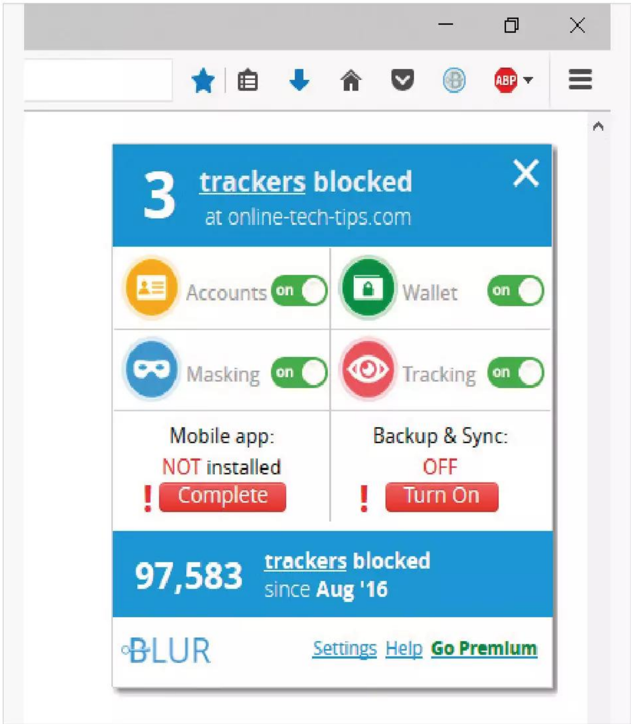
Make Windows better.

Give us feedback

TIP 5 Depending on the age of your computer, it's possible to create a boot password from the BIOS. You need to consult your motherboard manual as to how to accomplish this but you can set a password for being able to boot into your computer (before Windows even starts) and getting into the BIOS itself.

Enter Password

TIP 6 Consider installing several add-ons to your browser to improve its security and prevent any unwanted data miners or rogue scripts from being executed. Adblock Plus, Blur, No Script and other examples will secure your browsing session. For an extreme route, use the Tor browser.


3 trackers blocked at online-tech-tips.com

Accounts on

Wallet on

Masking on

Tracking on

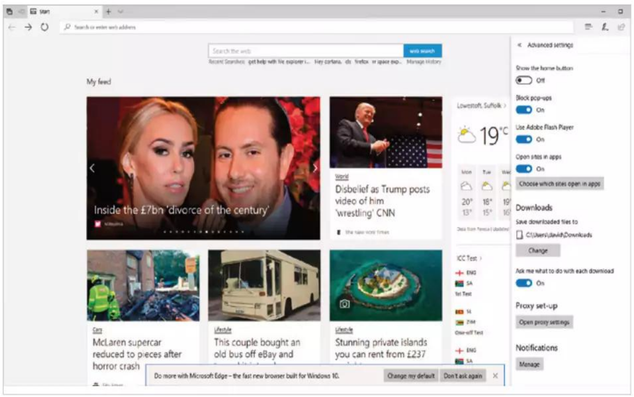
Mobile app: NOT installed

Backup & Sync: OFF

97,583 trackers blocked since Aug '16

ABP
Complete
Turn On
BLUR
Settings
Help
Go Premium

TIP 7 Flash and Java are superb entry points for malicious code to infect your computer and for snooping of various personal settings and data. Disabling both Java and Flash will prevent any such backdoors but limit your browsing experience on some sites.


Advanced settings

Show the home button: Off

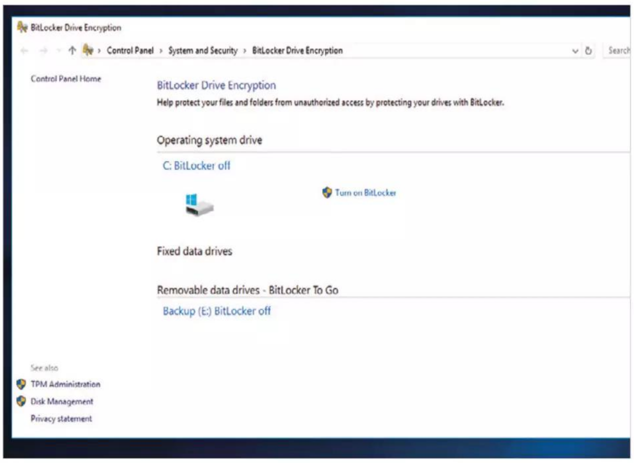
Block pop-ups: On

Use Adobe Flash Player: On

Open sites in apps: On

My feed
Inside the £7bn 'divorce of the century'
Disbelief as Trump posts video of him 'wrestling' CNN
19°C
McLaren supercar reduced to pieces after horror crash
This couple bought an old bus off eBay and
Stunning private islands you can rent from £237
Choose which sites open in apps
Downloads
Change
Proxy set-up
Open proxy settings
Notifications
Manage

TIP 8 Encrypting your installed hard drives and any external devices you use is an excellent way of securing your data and locking down Windows 10. Whilst it can be inconvenient, you can be safe in the knowledge that any lost data is virtually unhackable by all but the military supercomputers.


BitLocker Drive Encryption

Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.

Operating system drive

C: BitLocker off

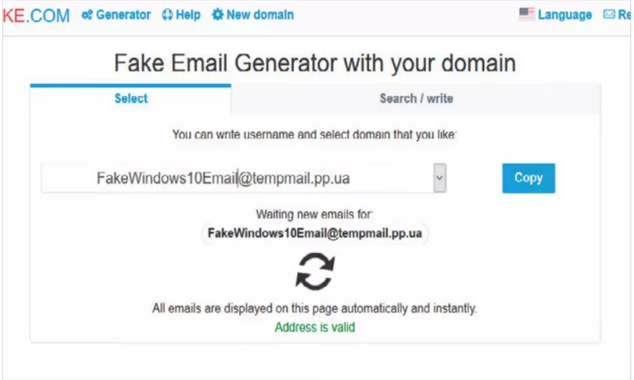
Fixed data drives

Removable data drives - BitLocker To Go

Backup (E:) BitLocker off

Control Panel › System and Security › BitLocker Drive Encryption
Control Panel Home
Turn on BitLocker
See also
TPM Administration
Disk Management
Privacy statement

TIP 9 Normally you'd use a valid email account to log into Windows 10, via an activated Microsoft account. However, consider setting up an alternative account that isn't linked to you. That way any data sent via Windows 10 to other sources won't contain any personal data.


Fake Email Generator with your domain

You can write username and select domain that you like:

FakeWindows10Email@tempmail.pp.ua

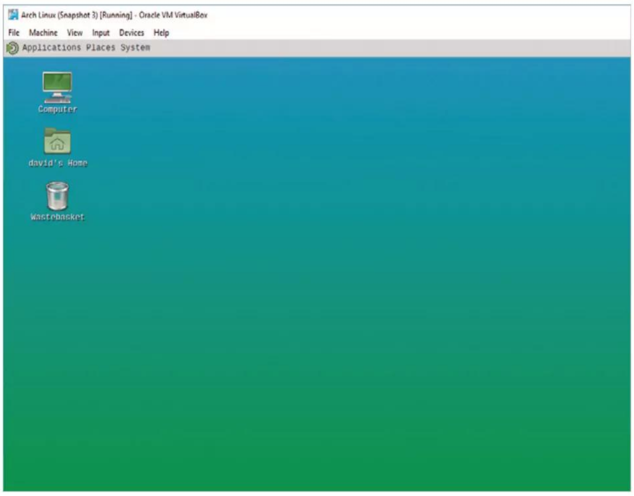
Waiting new emails for FakeWindows10Email@tempmail.pp.ua

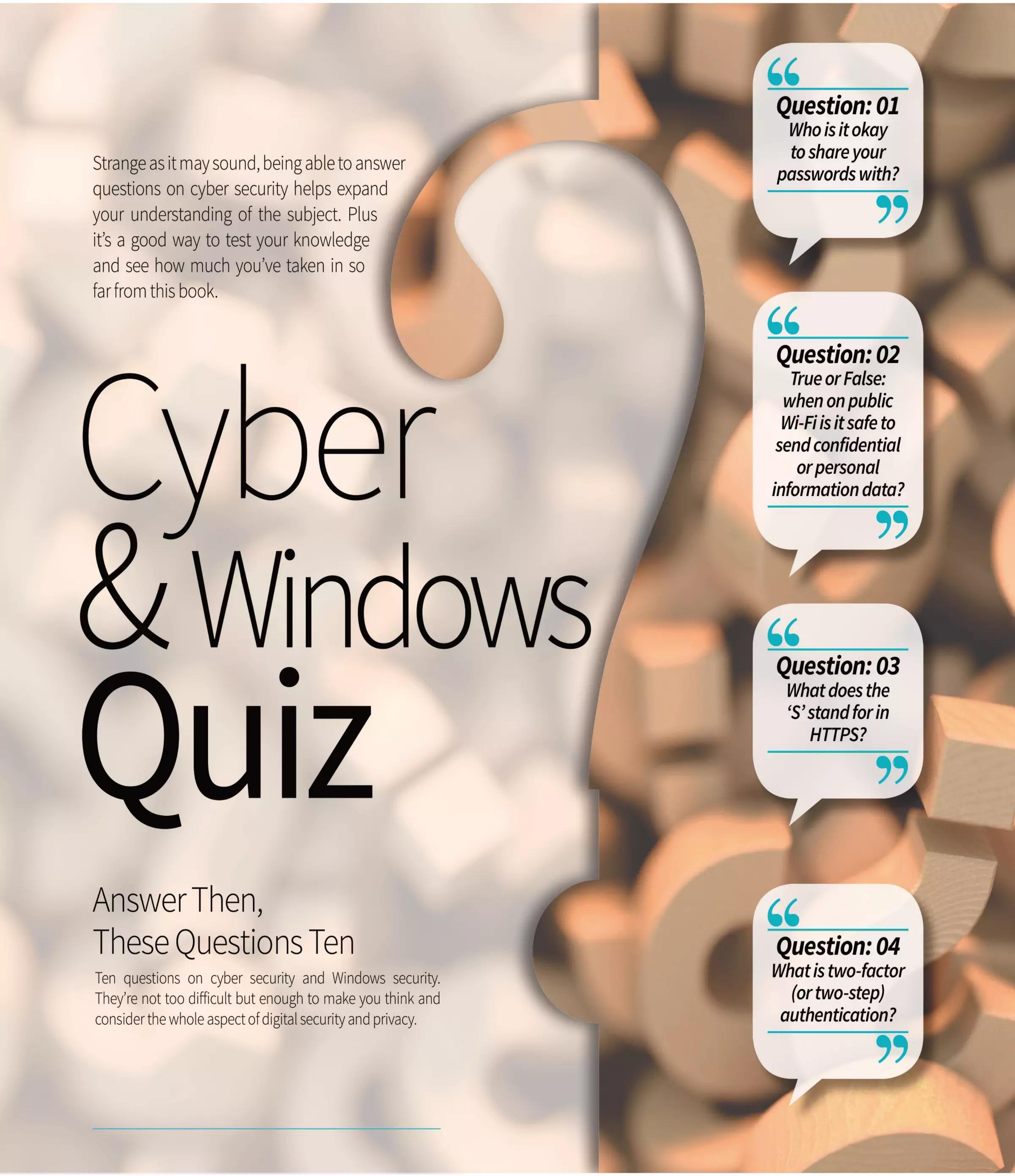
All emails are displayed on this page automatically and instantly.

Address is valid

KE.COM
Generator
Help
New domain
Language
Select
Search / write
Copy

TIP 10 Use a Virtual Machine within Windows 10 to conduct your day to day browsing and online work. The VM could be Windows 10 too or even adopt a more secure environment such as one of the higher-end security versions of Linux. Either way, a VM will be far more secure than Windows 10 on its own.


Arch Linux (Snapshot 3) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places System
Computer
david's Home
Wastebasket



Strange as it may sound, being able to answer questions on cyber security helps expand your understanding of the subject. Plus it's a good way to test your knowledge and see how much you've taken in so far from this book.

Cyber & Windows Quiz

Answer Then, These Questions Ten

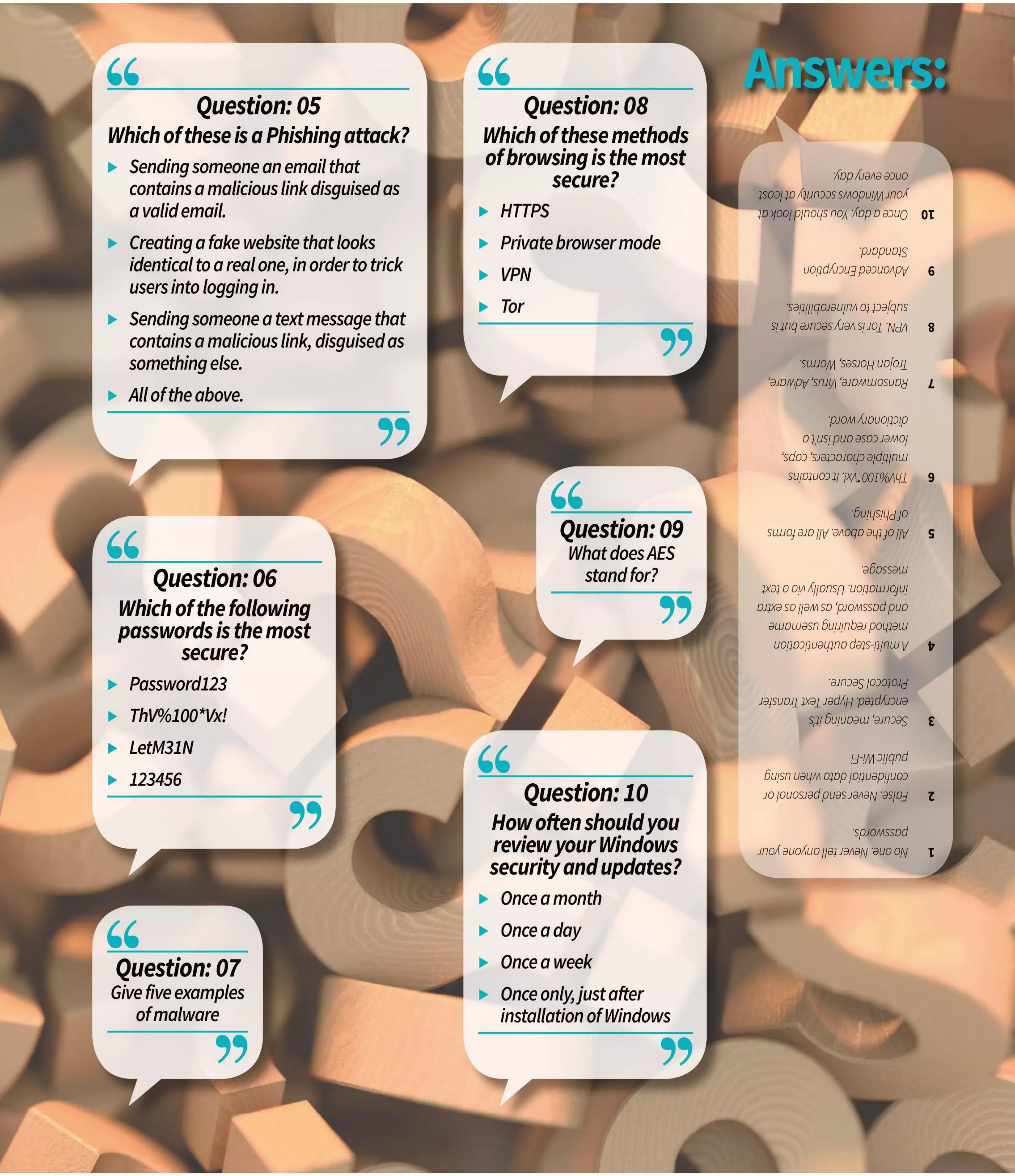
Ten questions on cyber security and Windows security. They're not too difficult but enough to make you think and consider the whole aspect of digital security and privacy.

Question: 01
Who is it okay to share your passwords with?

Question: 02
True or False: when on public Wi-Fi is it safe to send confidential or personal information data?

Question: 03
What does the 'S' stand for in HTTPS?

Question: 04
What is two-factor (or two-step) authentication?



Question: 05

Which of these is a Phishing attack?

- *Sending someone an email that contains a malicious link disguised as a valid email.*
- *Creating a fake website that looks identical to a real one, in order to trick users into logging in.*
- *Sending someone a text message that contains a malicious link, disguised as something else.*
- *All of the above.*

Question: 06

Which of the following passwords is the most secure?

- *Password123*
- *ThV%100*Vx!*
- *LetM31N*
- *123456*

Question: 07

Give five examples of malware

Question: 08

Which of these methods of browsing is the most secure?

- *HTTPS*
- *Private browser mode*
- *VPN*
- *Tor*

Question: 09

What does AES stand for?

Question: 10

How often should you review your Windows security and updates?

- *Once a month*
- *Once a day*
- *Once a week*
- *Once only, just after installation of Windows*

Answers:

1 *No one. Never tell anyone your passwords.*

2 *False. Never send personal or confidential data when using public Wi-Fi*

3 *Secure, meaning it's encrypted. Hyper Text Transfer Protocol Secure.*

4 *A multi-step authentication method requiring username and password, as well as extra information. Usually via a text message.*

5 *All of the above. All are forms of Phishing.*

6 *ThV%100*Vx!. It contains multiple characters, caps, lower case and isn't a dictionary word.*

7 *Ransomware, Virus, Adware, Trojan Horses, Worms.*

8 *VPN. Tor is very secure but is subject to vulnerabilities.*

9 *Advanced Encryption Standard.*

10 *Once a day. You should look at your Windows security at least once every day.*

What the Experts Say

Amongst the many quotes from security experts of the modern digital age, some stand out as either remarkably fortuitous or simply worth mentioning. We've compiled ten top quotes from the security world, that both entertain and make you think.

> “Relying on the government to protect your privacy is like asking a peeping tom to install your window blinds”

> “If you spend more on coffee than on IT security, you will be hacked. What's more, you deserve to be hacked.”

White House Cybersecurity Advisor, Richard Clarke.

> “Computer security can simply be protecting your equipment and files from disgruntled employees, spies and anything that goes bump in the night, but there is much more. Computer security makes sure no damage is done to your data and that no one is able to read it unless you want them to.”

Bruce Schneier, Protect Your Macintosh, 1994.

> “The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards.”

Gene Spafford.

“No serious commentary will say that the user has no responsibility. We all have responsibilities to lock our doors in our homes and to buckle up when we get in cars.”

Spokesman, Information Technology Association of America, Business Roundtable, AP, May 19, 2004.

“The condition of any backup is unknown until a restore is attempted.”

Schrodinger’s Backup.

“Phishing is a major problem because there really is no patch for human stupidity.”

Mike Danseglio, program manager in the Security Solutions group at Microsoft, April 4, 2006.

“If security were all that mattered, computers would never be turned on, let alone hooked into a network with literally millions of potential intruders.”

Dan Farmer, System Administrators Guide to Cracking.

“The whole notion of passwords is based on an oxymoron. The idea is to have a random string that is easy to remember. Unfortunately, if it’s easy to remember, it’s something non-random like ‘Susan’; and if it’s random, like ‘r7U2*Qnp,’ then it’s not easy to remember.”

Bruce Schneier.

“Like the death of a celebrity from a drug overdose, publicised data loss incidents remind us that we should probably do something about taking better care of our data. But we usually don’t, because we quickly remind ourselves that backups are boring as hell and that it’s shark week on Discovery.”

Nik Cubrilovic, TechCrunch.com, October 10, 2008.

“People often represent the weakest link in the security chain and are chronically responsible for the failure of security systems.”

Bruce Schneier, Secrets and Lies.

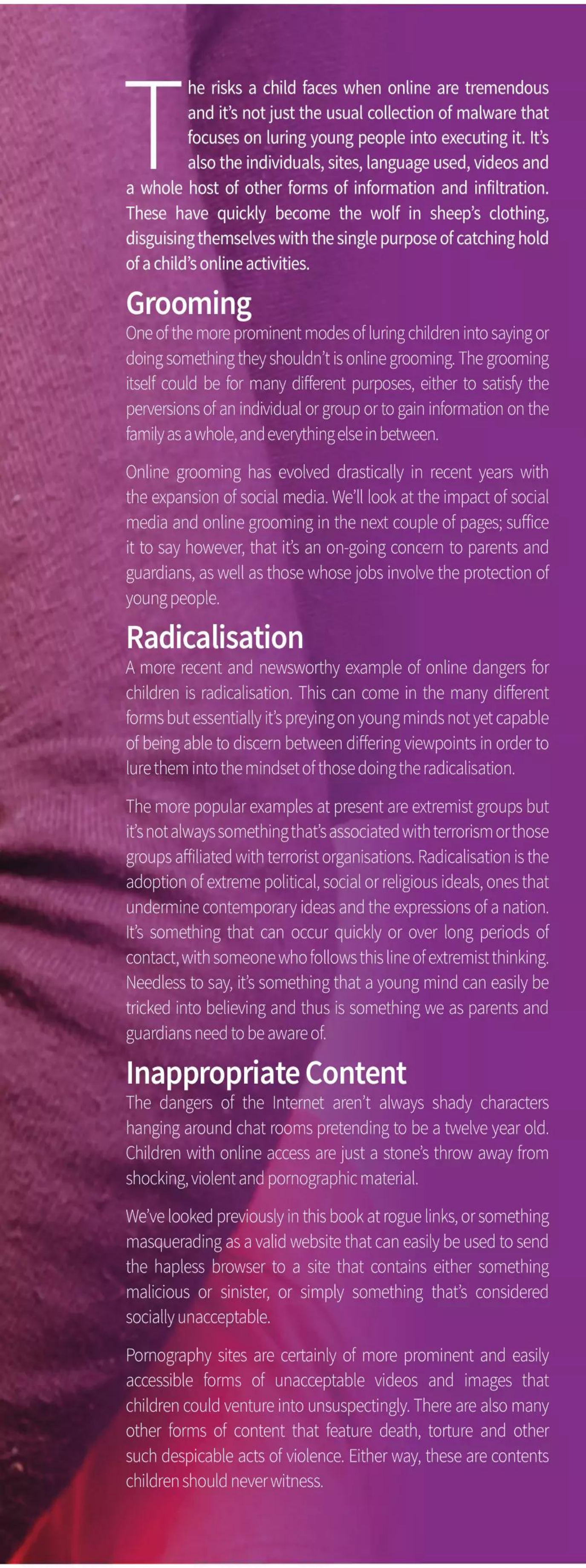
Online Child Protection

We as adults face numerous risks when online, children face significantly more. The predatory nature of some make the Internet an extremely hazardous place for a child to explore, despite the great benefits that it offers. The following pages will look at the risks involved for children when online but also how to prevent them and how to better protect your child while they navigate this virtual minefield.

132 Children Online: What are the Risks?
134 Social Media & Children
136 Search Engine Safety
138 Online Grooming
140 How Safe are the Sites Your Child Can Access?
142 Email and Child Safety
144 Top Child Friendly Email Programs and Services
146 Cyberbullying
148 How to Prevent and Deal with Cyberbullying
150 Helping Your Child Through the Internet
152 Your Child and Online Gaming, is it Safe?
154 Staying Safe when Gaming Online – Advice for Your Child
156 Monitoring What's Going On
158 Monitoring Online Activity for Non-Technical Guardians
160 Tips for Technical Guardians to Monitor a Child's Online Activity
162 Ten Monitoring Tools to Install and Use
164 Using the Windows Hosts File to Block Sites

Children Online: **What are the Risks?**

Every parent or guardian knows that being online represents an entirely new frontier of potential dangers for young children and teens. These dangers come in many forms, with each being capable of greatly affecting the lives of all involved.



The risks a child faces when online are tremendous and it's not just the usual collection of malware that focuses on luring young people into executing it. It's also the individuals, sites, language used, videos and a whole host of other forms of information and infiltration. These have quickly become the wolf in sheep's clothing, disguising themselves with the single purpose of catching hold of a child's online activities.

Grooming

One of the more prominent modes of luring children into saying or doing something they shouldn't is online grooming. The grooming itself could be for many different purposes, either to satisfy the perversions of an individual or group or to gain information on the family as a whole, and everything else in between.

Online grooming has evolved drastically in recent years with the expansion of social media. We'll look at the impact of social media and online grooming in the next couple of pages; suffice it to say however, that it's an on-going concern to parents and guardians, as well as those whose jobs involve the protection of young people.

Radicalisation

A more recent and newsworthy example of online dangers for children is radicalisation. This can come in the many different forms but essentially it's preying on young minds not yet capable of being able to discern between differing viewpoints in order to lure them into the mindset of those doing the radicalisation.

The more popular examples at present are extremist groups but it's not always something that's associated with terrorism or those groups affiliated with terrorist organisations. Radicalisation is the adoption of extreme political, social or religious ideals, ones that undermine contemporary ideas and the expressions of a nation. It's something that can occur quickly or over long periods of contact, with someone who follows this line of extremist thinking. Needless to say, it's something that a young mind can easily be tricked into believing and thus is something we as parents and guardians need to be aware of.

Inappropriate Content

The dangers of the Internet aren't always shady characters hanging around chat rooms pretending to be a twelve year old. Children with online access are just a stone's throw away from shocking, violent and pornographic material.

We've looked previously in this book at rogue links, or something masquerading as a valid website that can easily be used to send the hapless browser to a site that contains either something malicious or sinister, or simply something that's considered socially unacceptable.

Pornography sites are certainly of more prominent and easily accessible forms of unacceptable videos and images that children could venture into unsuspectingly. There are also many other forms of content that feature death, torture and other such despicable acts of violence. Either way, these are contents children should never witness.

Cyber Bullying

Cyber bullying comes from many diverse sources on the Internet. It's not simply others at school bullying someone on Facebook, Twitter etc., there are some startling statistics that detail the kind of bullying that occurs in online gaming.

For example, leading anti-bulling charity Ditch the Label, recently reported on a sample of 2,500 young people aged between 12 and 26. The report discovered that 64 percent were trolled whilst playing an online game; 57 percent experienced some form of bullying; half experienced hate speech and threats of violence; 39 percent received unwanted sexual contac;, 34 percent had private information shared; and 38 percent had been hacked whilst playing.

With comments such as 'I hope your parents die' and 'I'm coming to kill you', and children not being able to process this kind of violence, cyber bullying whilst playing online games is certainly an issue that needs addressing.

Identity Theft

Possibly used as part of grooming in order to gain information from a child, identity theft is a growing concern. Keeper Security, a leading password management app, recently published an infographic on web security. According to the company's sources, children are thirty five times more likely to have their identities stolen, with an estimated 1.3 million children affected each year by identity theft and nearly half of them under the age of six.

It's a shocking statistic and one that can lessened through online education and not leaving a child alone in front of the Internet; both not always easy to accomplish but also not impossible.

Online Scams

Children are vulnerable to varying forms of online scams purely due to their, in some ways, innocence and lack of experience, as well as acceptability of what they read to be a fact or truth. It's therefore quite easy to dupe a young person into a scam that either tries to take money from them, or some form of personal information.

The likely scams that children often fall for are usually related to gaming, i.e. 'click here to win 1000 in gold' 'get extra lives' or something that gives them an advantage in the latest game. Often scams will involve having them click a link that's offering to sell the latest games console, football kit, phones and other technology, all at unbelievably low prices. Naturally it's all fake but to a child it's an offer that's hard to refuse.

These are just some examples of what's out there and what lies in wait for a young person with an inquisitive mind and a trigger-happy mouse button. These individuals and groups have designed their risks to target children in particular, so we need to make doubly sure that when online our children are as educated, savvy and safe as possible.

> Whilst the Internet and all its contents are an incredible learning resource that can bring
>
> “
>
> ***Online Risks***
>
> ”
>
> together people from all over the world, inevitably there will be those who wish to exploit some of the most vulnerable among us, children and young people.

Social Media and Children

The impact of social media on children has been the subject of numerous reports over the last few years. With more and more children and young people gaining access to Facebook, Twitter, WhatsApp, Instagram and so on, there's a growing concern as to how it's affecting online safety.

Any site or portal where some form of social interaction occurs can be classed as social media, so even if you don't allow your children access to Facebook et al, there's still a chance they're in contact via gaming or an app of some description: YouTube, blogs and so on.

Reports from the American Academy of Paediatrics has found that using social media does provide benefits for young people. According to findings, regular use of social media platforms enhances communication, social connections and technical skills. Not only that, it allows young people to connect with extended family members and friends they won't see for perhaps years at a time, as they live in places they're not likely to visit. Depending on the content, social media can help a young person develop better perspectives on various issues in the media and when talked about with an adult, they can begin to form their own opinions, an impressive stage in a young person's life.

In some ways social media can help a young person express their inner feelings and encourages freedom of thought and engagement with similar age people. There's potential for a young person to learn new things, whether that's simple life hacks or discovering someone's job role. All in all, it adds up, on paper at least, to a positive experience that can greatly help a young person grow and help them form a more mature understanding of the world around them; something we didn't have before the Internet.

Sadly, with every positive aspect there are several negatives. Whilst the effects of social media on a child can be for good, they are mostly overshadowed by the popular negative aspects that ultimately rise to the surface. The sheer vastness of social media is one of the main causes for such negativity. Due to its freedom and limitless potential, there's no definable control on the scope of information. Yes, the social media platform can apply rules, filters and restrictions but these seem to be far too easily bypassed, and to some degree worthless in the end.

Cyber bullying is rife on social media. From threats made to young people, to digs at their appearance and body shaming, it's a platform that has quickly devolved into a pit of despair and depression for some unfortunate youngsters. This can lead, in extreme cases, to fatal consequences but generally the collective term for the negativity plied upon the youth of today is 'Facebook Depression'.

In recent months, the Royal Society for Public Health together with the Young Health Movement released a survey that revealed Instagram to have the negative impact on a young person's mental wellbeing, accusing the media platform of deepening young people's feelings of inadequacy and anxiety. It's a disturbing fact that on top of the pressures of school or college life, young people are having to put themselves through the mill whilst simply sitting in front of a screen.

Mental health is a major concern amongst young people but social media also presents its darker side through online grooming, potential radicalisation and the spread of malware. Each of these will greatly affect a young person and can lead to higher levels of anxiety, depression and withdrawal. For example, the spread of malware may not sound too negative on the wellbeing of a young person but put yourself in the place of the child who has unwittingly executed some form of malware on the family computer or the school network. The negative emotional effects from this happening can be huge to someone whose immaturity can't deal with the aftereffects.

The safety side of social media and children comes in many forms then. Mental health concerns, access to inappropriate content, Internet borne digital threats, bullying, grooming, loneliness and body image. Where it's easy to point out the risks of Internet stranger danger, it's not always easy to cover what happens should someone post edited and manipulated images of a young person to social media.

Therefore, the pressure on parents and guardians is just as immense, when helping our young people navigate the digital wild west frontier that is social media.

Using social media is amongst the most common online activities of the modern day young person. The likes of Facebook, Twitter, Instagram and many more all contribute to the billions of hours collectively spent via computers and mobile devices, with online gaming quickly following on the heels of the more popular social media portals.

> **“*Safe Social Media*”**

Search Engine Safety

The search engine is the portal into the wider Internet and through it we can view everything from man's first steps on the moon, to extremist group propaganda videos. It's therefore paramount that children are aware of the dangers of the search engine.

While the Google search portal isn't dangerous in itself, it's what potentially lies behind the search entered that makes it such a dangerous place for young people to venture into. Many young people are somewhat more tech-savvy than most adults but the younger children are at risk from a seemingly innocent search resulting in inappropriate content being displayed.

> **"*Safer Searching*"**

It doesn't take much imagination to consider how a particular scenario may be played out. A child is left in front of a search engine, they enter something to do with a school project on World War 2 and start to follow the links. Although part of history, some of the images that may be displayed could be deemed inappropriate to a primary school child, or those as young. To expand, what if the child then follows links to modern day warfare and from there potentially to videos depicting extreme violence. That then can snowball into accessing what can only be described as the real nasty stuff, which isn't something any child should ever witness.

The above scenario is, of course, the extreme end of what could potentially happen. Without going down the fearmongering road, the search engine can lead someone unsuspecting into a whole heap of trouble. That trouble can come from school, your ISP should any illegally hosted content be accessed, or even from accessing malware, so it's worth making sure that whatever search engine you use, any filters are currently set to On or Strict and it's recommended that you don't leave a child alone in front of a search engine for any length of time.

If you consider Google to be too risky, there are the likes of DuckDuckGo, a search engine that not only protects your data by not logging any searches but also features an extensive filter engine. Likewise StartPage, Bing, Boardreader and CC Search can also fulfil most users' requirements whilst filtering inappropriate content and allowing a higher degree of Internet privacy.

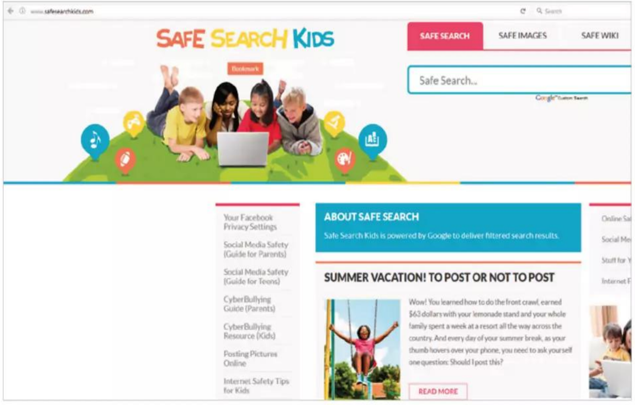
Alternatively there are steps we as parents, adults and guardians can do to help prevent any inappropriate content from appearing in a search result. There are numerous sites that have been designed specifically for safer searching with children in mind. The strict search policies of an engine may be good but there's always a chance that something could get through the net and reveal itself on the screen.

Six Safe Search Sites

Therefore, here are six child safe search engines. The age ranges vary but generally they're pitching to primary or low-middle school children. Either way, they're certainly worth considering and bookmarking for when a child is using the computer for school or general research.

SAFE SEARCH KIDS

A UK-based search engine that utilises Google's SafeSearch technology and provides a friendly front end. It's a good starting point and one that doesn't display picture icons along with search results; thus eliminating any inappropriate images that may unintentionally slip through.


SAFE SEARCH KIDS
SAFE SEARCH
SAFE IMAGES
SAFE WIKI
Safe Search...
Bookmark
Your Facebook Privacy Settings
Social Media Safety (Guide for Parents)
Social Media Safety (Guide for Teens)
CyberBullying Guide (Parents)
CyberBullying Resource (Kids)
Posting Pictures Online
Internet Safety Tips for Kids
READ MORE

ABOUT SAFE SEARCH

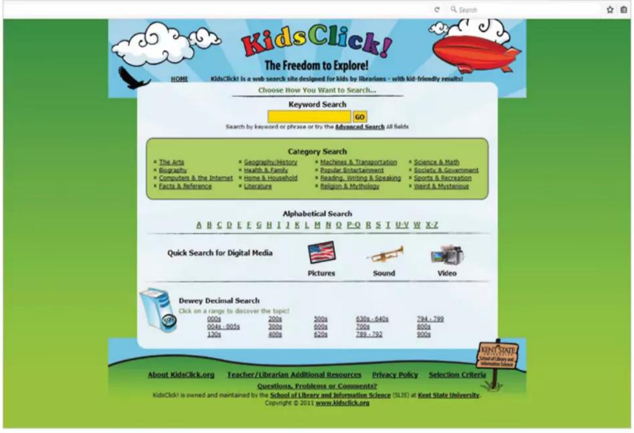
Safe Search Kids is powered by Google to deliver filtered search results.

SUMMER VACATION! TO POST OR NOT TO POST

Wow! You learned how to do the front crawl, earned $63 dollars with your lemonade stand and your whole family spent a week at a resort all the way across the country. And every day of your summer break, as your thumb hovers over your phone, you need to ask yourself one question: Should I post this?

KIDSCLICK

KidsClick is a search engine designed and created by librarians for children who are searching for school related research. Each result returned features a description and reading level, along with suggestions and homework helpers.

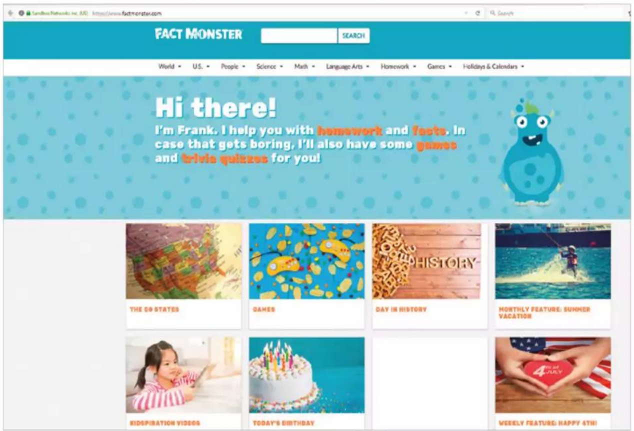

KidsClick!
The Freedom to Explore!
HOME
Choose How You Want to Search...
Keyword Search
GO
Category Search
Alphabetical Search
A B C D E F G H I J K L M N O P-Q R S T U-V W X-Z
Quick Search for Digital Media
Pictures
Sound
Video
Dewey Decimal Search
About KidsClick.org
Teacher/Librarian Additional Resources
Privacy Policy
Selection Criteria
Questions, Problems or Comments?

KidsClick! is a web search site designed for kids by librarians - with kid-friendly results!

KidsClick! is owned and maintained by the School of Library and Information Science (SLIS) at Kent State University.

FACT MONSTER

Fact Monster is an excellent site that's dedicated to helping children research school topics. It's a free online almanac, dictionary, encyclopaedia and thesaurus and is aimed at children between the ages of eight and fourteen.

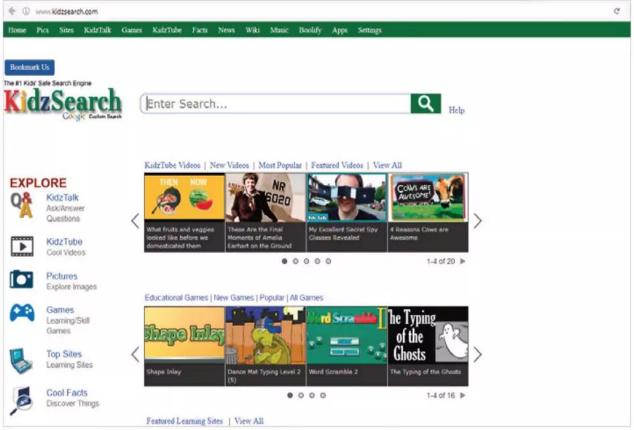

FACT MONSTER
SEARCH
World
U.S.
People
Science
Math
Language Arts
Homework
Games
Holidays & Calendars
HISTORY
THE 50 STATES
GAMES
DAY IN HISTORY
MONTHLY FEATURE: SUMMER VACATION
INSPIRATION VIDEOS
TODAY'S BIRTHDAY
WEEKLY FEATURE: HAPPY 4TH!

Hi there!

I'm Frank. I help you with homework and facts. In case that gets boring, I'll also have some games and trivia quizzes for you!

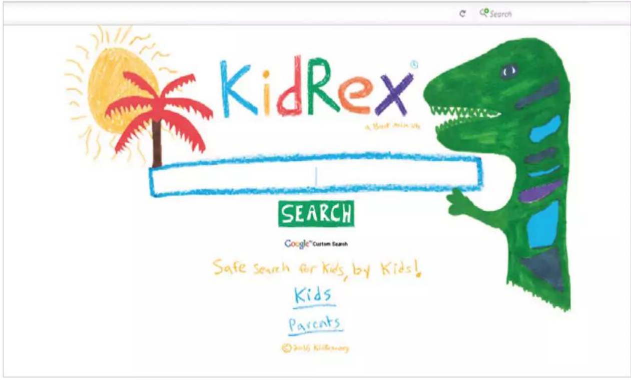
KIDZSEARCH

Here's another customised search engine utilising Google's SafeSearch strict results filter. Additionally, it also features a banned keyword search system that will not return any results from the black list of banned words.


www.kidzsearch.com
Home
Pics
Sites
KidzTalk
Games
KidzTube
Facts
News
Wiki
Music
Boolify
Apps
Settings
Bookmark Us
The #1 Kids' Safe Search Engine
KidzSearch
Enter Search...
Help
EXPLORE
KidzTalk
Ask/Answer Questions
KidzTube
Cool Videos
Pictures
Explore Images
Games
Learning/Skill Games
Top Sites
Learning Sites
Cool Facts
Discover Things
KidzTube Videos | New Videos | Most Popular | Featured Videos | View All
Educational Games | New Games | Popular | All Games
Shape Inlay
The Typing of the Ghosts
Word Scramble 2
Featured Learning Sites | View All

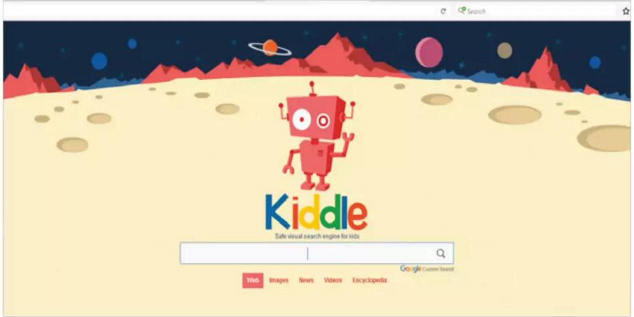
KIDREX

A simple site that's designed for much younger users. KidRex is powered by Google's own search engine but as you'd expect, filters out any inappropriate content. Further more, as a parent, you're also able to customise the filters to ensure safer or less restrictive search results.


KidRex
SEARCH
Google Custom Search
Safe Search for Kids, by Kids!
Kids
Parents

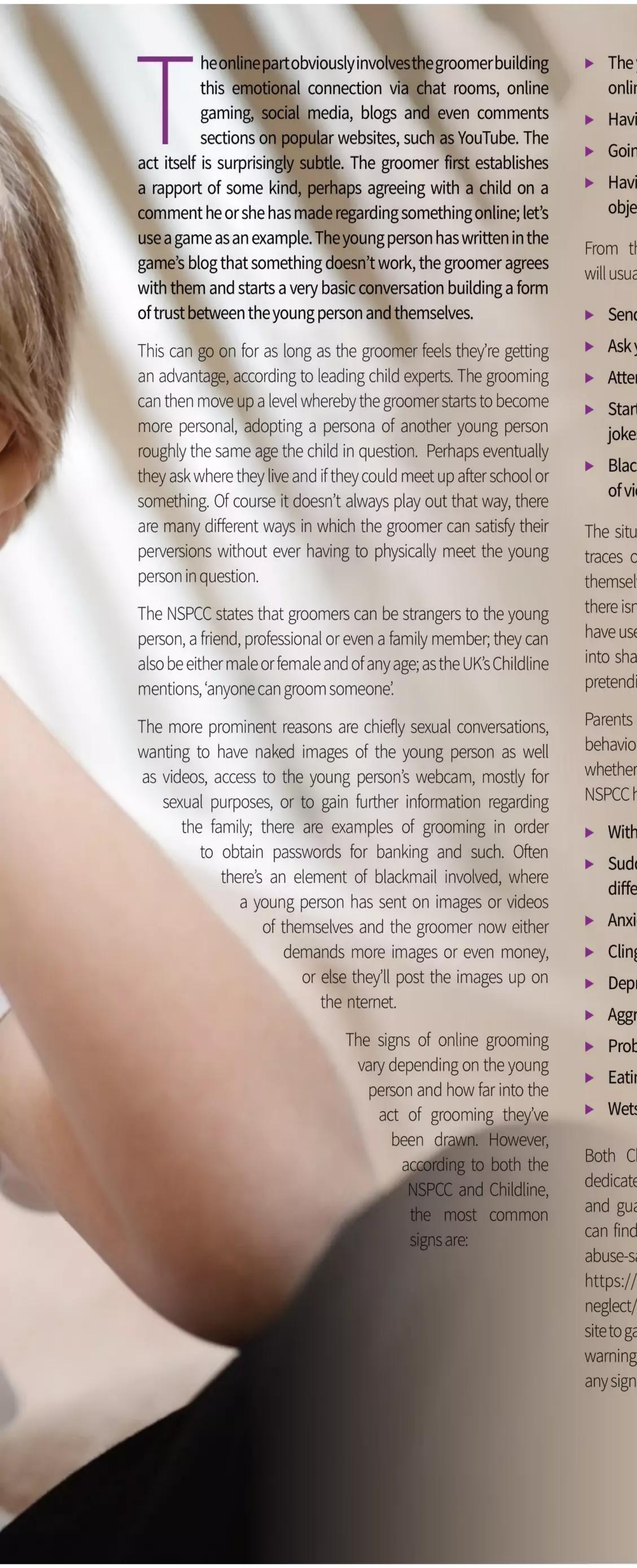
KIDDLE

A great and friendly search engine for children and young people. Kiddle provides strict filtering along with child-friendly results that are grouped by those deemed safe and handpicked by the Kiddle editors. Here are trusted sites that aren't specifically written for children but provide understandable content and safe famous sites, that are harder to understand but still relevant.


Kiddle
Safe visual search engine for kids
Web
Images
News
Videos
Encyclopedia

Online Grooming

Of all the many despicable acts and threats that arise on the Internet toward young people, online grooming is undoubtedly one of the worst examples. It's a tricky act to confirm at times too, as those who groom often cleverly hide their tracks but it is possible to spot signs of it happening.



The online part obviously involves the groomer building this emotional connection via chat rooms, online gaming, social media, blogs and even comments sections on popular websites, such as YouTube. The act itself is surprisingly subtle. The groomer first establishes a rapport of some kind, perhaps agreeing with a child on a comment he or she has made regarding something online; let's use a game as an example. The young person has written in the game's blog that something doesn't work, the groomer agrees with them and starts a very basic conversation building a form of trust between the young person and themselves.

This can go on for as long as the groomer feels they're getting an advantage, according to leading child experts. The grooming can then move up a level whereby the groomer starts to become more personal, adopting a persona of another young person roughly the same age the child in question. Perhaps eventually they ask where they live and if they could meet up after school or something. Of course it doesn't always play out that way, there are many different ways in which the groomer can satisfy their perversions without ever having to physically meet the young person in question.

The NSPCC states that groomers can be strangers to the young person, a friend, professional or even a family member; they can also be either male or female and of any age; as the UK's Childline mentions, 'anyone can groom someone'.

The more prominent reasons are chiefly sexual conversations, wanting to have naked images of the young person as well as videos, access to the young person's webcam, mostly for sexual purposes, or to gain further information regarding the family; there are examples of grooming in order to obtain passwords for banking and such. Often there's an element of blackmail involved, where a young person has sent on images or videos of themselves and the groomer now either demands more images or even money, or else they'll post the images up on the nternet.

The signs of online grooming vary depending on the young person and how far into the act of grooming they've been drawn. However, according to both the NSPCC and Childline, the most common signs are:

- The young person being very secretive, including their online activity.
- Having older boyfriends or girlfriends.
- Going to unusual places to meet up with friends.
- Having new things such as clothes, phones or other objects they can't readily explain.

From the perspective of the young person, a groomer will usually:

- Send you lots of private messages.
- Ask you to keep conversations a secret.
- Attempt to find out more about you and your family.
- Start to send you sexual messages, usually starting with jokes then moving on.
- Blackmail you into sending images or videos by threats of violence to you or your family.

The situations can vary and the groomer is adept at hiding traces of their activity as well as lying to someone about themselves. Childline states: "It's important to remember that there isn't one type of groomer. Many different kinds of people have used the Internet to trick, force or persuade young people into sharing sexual images of themselves. Often it's an adult pretending to be a young person, but not always."

Parents and guardians can watch out for certain types of behaviour, which could be signs of grooming, regardless of whether it's online, via a phone chat app or even in person. The NSPCC have listed the following as potential signs:

- Withdrawn
- Suddenly behaves differently
- Anxious
- Clingy
- Depressed
- Aggressive
- Problems sleeping
- Eating disorders
- Wets the bed
- Soils clothes
- Takes risks
- Misses school
- Changes in eating habits
- Obsessive behaviour
- Nightmares
- Drugs
- Alcohol
- Self-harm
- Thoughts about suicide

Both Childline and the NSPCC have excellent websites dedicated to online grooming, along with advice to both parents and guardians, as well as young people and children. You can find them at https://childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/online-grooming/#10 and https://nspcc.org.uk/preventing-abuse/child-abuse-and-neglect/grooming/. It's certainly worth reading through each site to gain a better understanding of online grooming, what the warning signs are and how to support a young person should any signs be apparent.

“What it is and what to Look Out for”

The NSPCC (the National Society for the Prevention of Cruelty to Children) defines grooming as when someone builds an emotional connection with a child to gain their trust for the purposes of sexual abuse, sexual exploitation or trafficking.

How Safe are the Sites Your Child Can Access?

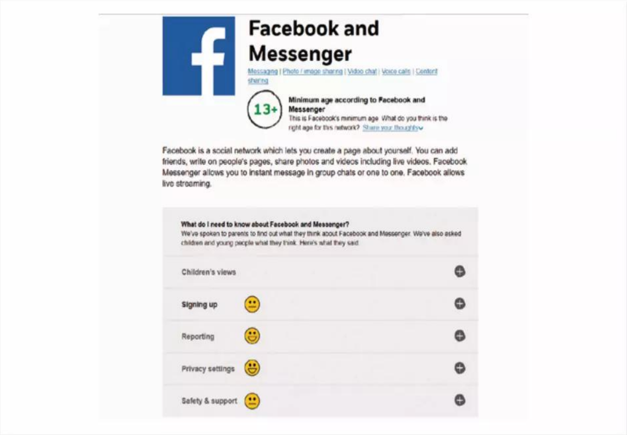
Mobile operator O2, YouGov and the NSPCC have teamed up with Net Aware to create a site that reviews popular sites and apps that children and young people use. This guide allows parents and guardians to view the information to help them understand their child's online world.

Net Aware

Net Aware is an excellent site, and can be found at https://net-aware.org.uk/. Within you can find an A to Z of Most Popular sites and how safe they actually are according to face icons. Here are ten of the popular choices with their safety information.

FACEBOOK AND MESSENGER

Facebook has gone to great lengths in recent years to ensure a higher degree of safety. There's a lot of ground left to cover but from the point of view of Net Aware, it's about average in terms of safety. Signing up and Safety & Support need looking into however.



Facebook and Messenger

Messaging | Photo / image sharing | Video chat | Voice calls | Content sharing

13+ **Minimum age according to Facebook and Messenger**
This is Facebook's minimum age. What do you think is the right age for this network? Share your thoughts

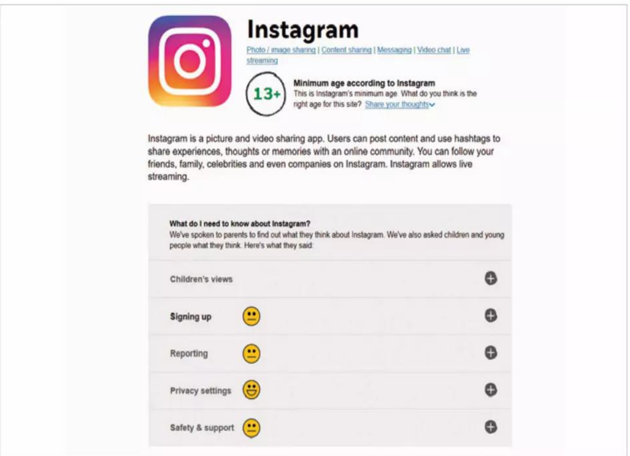
Facebook is a social network which lets you create a page about yourself. You can add friends, write on people's pages, share photos and videos including live videos. Facebook Messenger allows you to instant message in group chats or one to one. Facebook allows live streaming.

What do I need to know about Facebook and Messenger?
We've spoken to parents to find out what they think about Facebook and Messenger. We've also asked children and young people what they think. Here's what they said

Children's views ⊕
Signing up 😐 ⊕
Reporting 🙂 ⊕
Privacy settings 🙂 ⊕
Safety & support 😐 ⊕

INSTAGRAM

Instagram only manages to gain an upvote (smiley face) in the Privacy Settings section, with more rigid controls being asked for from parents and carers with regards to Signing Up, Safety & Support and Reporting.



Instagram

Photo / image sharing | Content sharing | Messaging | Video chat | Live streaming

13+ **Minimum age according to Instagram**
This is Instagram's minimum age. What do you think is the right age for this site? Share your thoughts

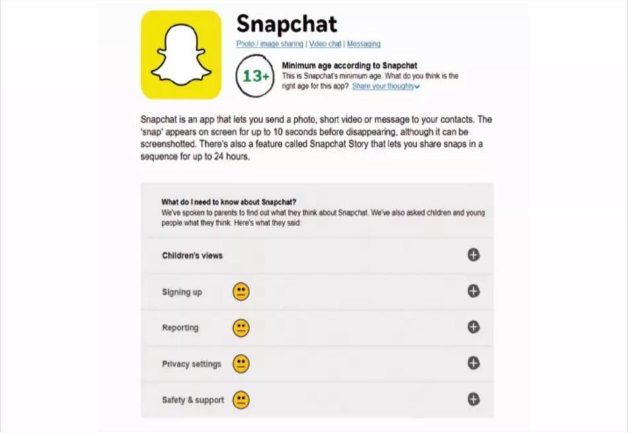
Instagram is a picture and video sharing app. Users can post content and use hashtags to share experiences, thoughts or memories with an online community. You can follow your friends, family, celebrities and even companies on Instagram. Instagram allows live streaming.

What do I need to know about Instagram?
We've spoken to parents to find out what they think about Instagram. We've also asked children and young people what they think. Here's what they said

Children's views ⊕
Signing up 😐 ⊕
Reporting 😐 ⊕
Privacy settings 🙂 ⊕
Safety & support 😐 ⊕

SNAPCHAT

According to Net Aware, 32% of children and young people who reviewed Snapchat thought that it can be risky. There aren't any 'happy face' icons among the sections, so be wary of how it works.



Snapchat

Photo / image sharing | Video chat | Messaging

13+ **Minimum age according to Snapchat**
This is Snapchat's minimum age. What do you think is the right age for this app? Share your thoughts

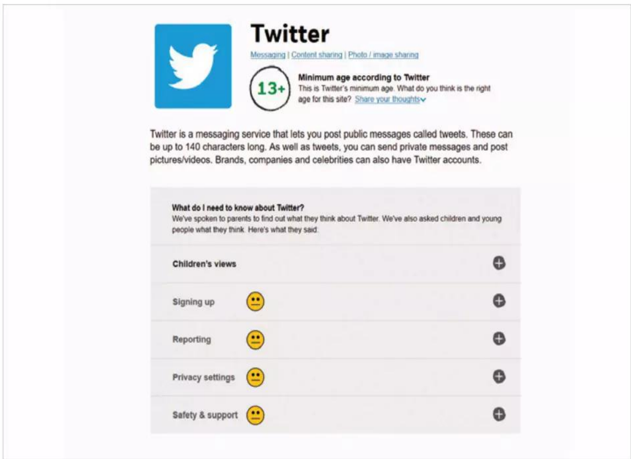
Snapchat is an app that lets you send a photo, short video or message to your contacts. The 'snap' appears on screen for up to 10 seconds before disappearing, although it can be screenshotted. There's also a feature called Snapchat Story that lets you share snaps in a sequence for up to 24 hours.

What do I need to know about Snapchat?
We've spoken to parents to find out what they think about Snapchat. We've also asked children and young people what they think. Here's what they said:

Children's views ⊕
Signing up 😐 ⊕
Reporting 😐 ⊕
Privacy settings 😐 ⊕
Safety & support 😐 ⊕

TWITTER

Some of the major concerns regarding Twitter are: uncontrolled Tweets, fake and scam tweets and abusive behaviour. It doesn't rate too highly, on a par with Snapchat, so it's worth reading through the available content prior to signing up or allowing a young person to sign up.



Twitter

Messaging | Content sharing | Photo / image sharing

13+ **Minimum age according to Twitter**
This is Twitter's minimum age. What do you think is the right age for this site? Share your thoughts

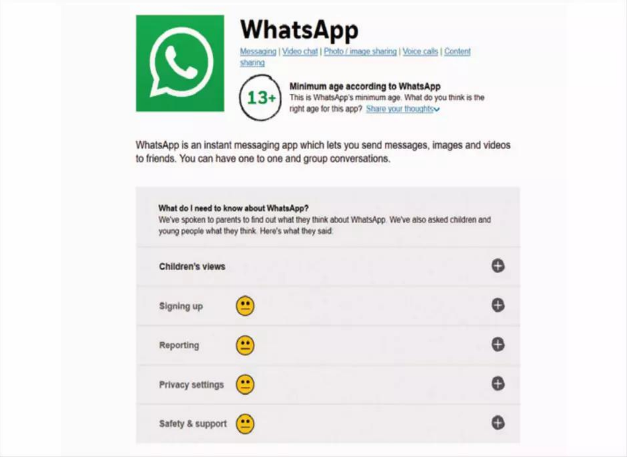
Twitter is a messaging service that lets you post public messages called tweets. These can be up to 140 characters long. As well as tweets, you can send private messages and post pictures/videos. Brands, companies and celebrities can also have Twitter accounts.

What do I need to know about Twitter?
We've spoken to parents to find out what they think about Twitter. We've also asked children and young people what they think. Here's what they said.

Children's views ⊕
Signing up 😐 ⊕
Reporting 😐 ⊕
Privacy settings 😐 ⊕
Safety & support 😐 ⊕

WHATSAPP

Another not too highly rated site, WhatsApp raises several concerns over ability to be contacted by strangers, random people being able to view your profile picture and the potential for receiving scam messages.



WhatsApp

Messaging | Video chat | Photo / image sharing | Voice calls | Content sharing

13+ **Minimum age according to WhatsApp**
This is WhatsApp's minimum age. What do you think is the right age for this app? Share your thoughts

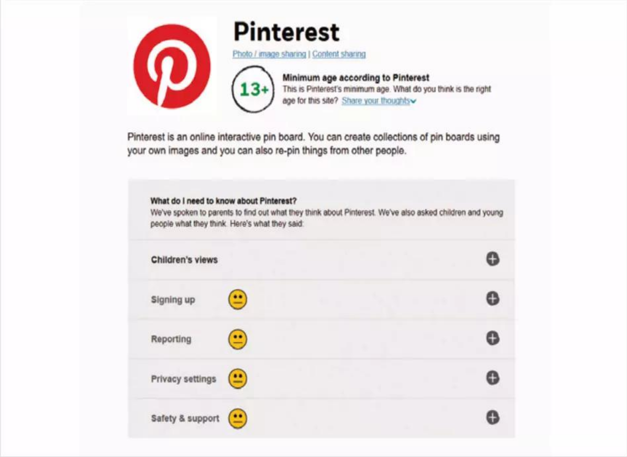
WhatsApp is an instant messaging app which lets you send messages, images and videos to friends. You can have one to one and group conversations.

What do I need to know about WhatsApp?
We've spoken to parents to find out what they think about WhatsApp. We've also asked children and young people what they think. Here's what they said.

Children's views ⊕
Signing up 😐 ⊕
Reporting 😐 ⊕
Privacy settings 😐 ⊕
Safety & support 😐 ⊕

PINTEREST

The main concern with Pinterest is that young people and children can't always control what they see, which means there are times when inappropriate content can be viewed by minors. Again, Net Aware rate it the same as YouTube, Snapchat and Twitter.



Pinterest

Photo / image sharing | Content sharing

13+ **Minimum age according to Pinterest**
This is Pinterest's minimum age. What do you think is the right age for this site? Share your thoughts

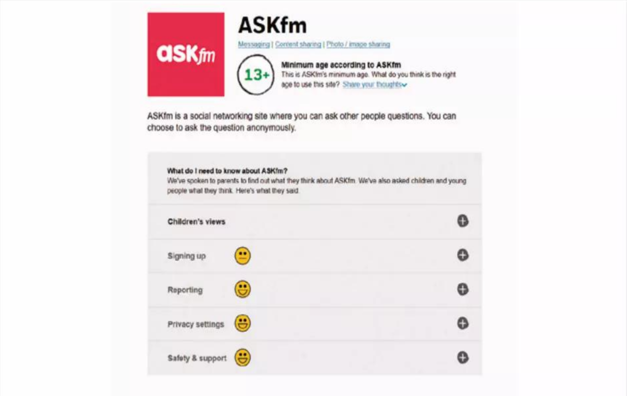
Pinterest is an online interactive pin board. You can create collections of pin boards using your own images and you can also re-pin things from other people.

What do I need to know about Pinterest?
We've spoken to parents to find out what they think about Pinterest. We've also asked children and young people what they think. Here's what they said:

Children's views ⊕
Signing up 😐 ⊕
Reporting 😐 ⊕
Privacy settings 😐 ⊕
Safety & support 😐 ⊕

ASKFM

This is a social networking site where you can ask other people questions, anonymously if you want to. The anonymity raises concerns, along with instances of bullying and trolling, as well as possible exposure to inappropriate content. However, it does have the highest 'face' rating off all the apps so far.



ASKfm

Messaging | Content sharing | Photo / image sharing

13+ **Minimum age according to ASKfm**
This is ASKfm's minimum age. What do you think is the right age to use this site? Share your thoughts

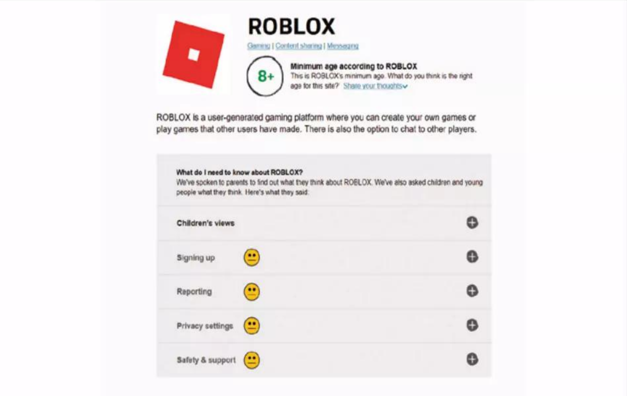
ASKfm is a social networking site where you can ask other people questions. You can choose to ask the question anonymously.

What do I need to know about ASKfm?
We've spoken to parents to find out what they think about ASKfm. We've also asked children and young people what they think. Here's what they said.

Children's views ⊕
Signing up 😐 ⊕
Reporting 😃 ⊕
Privacy settings 😃 ⊕
Safety & support 😃 ⊕

ROBLOX

This is an online game where you're able to play games created by others, or create games yourself. Whilst fun, it does have issues whereby users can add you to their friends list and communicate with you and it features in-app purchasing, which can be difficult to manage for parents and guardians.



ROBLOX

Gaming | Content sharing | Messaging

8+ **Minimum age according to ROBLOX**
This is ROBLOX's minimum age. What do you think is the right age for this site? Share your thoughts

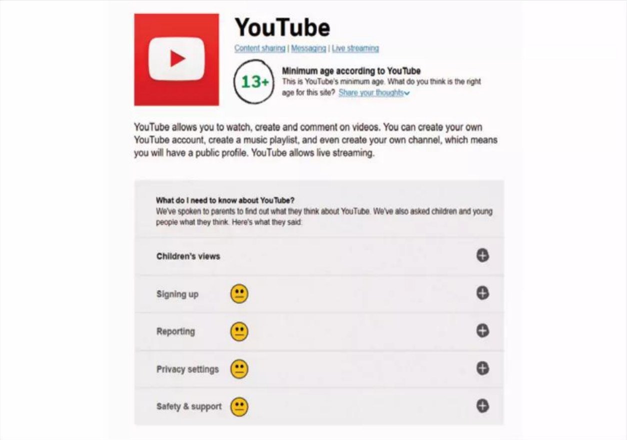
ROBLOX is a user-generated gaming platform where you can create your own games or play games that other users have made. There is also the option to chat to other players.

What do I need to know about ROBLOX?
We've spocken to parents to find out what they think about ROBLOX. We've also asked children and young people what they think. Here's what they said:

Children's views ⊕
Signing up 😐 ⊕
Reporting 😐 ⊕
Privacy settings 😐 ⊕
Safety & support 😐 ⊕

YOUTUBE

YouTube's infamous use by extremist groups when posting inappropriate videos is by far one of the most negative aspects of its use among young people. Examples of abusive comments and possibly inappropriate adverts are concerns too. Net Aware rates it on a par with Snapchat and Twitter.



YouTube

Content sharing | Messaging | Live streaming

13+ **Minimum age according to YouTube**
This is YouTube's minimum age. What do you think is the right age for this site? Share your thoughts

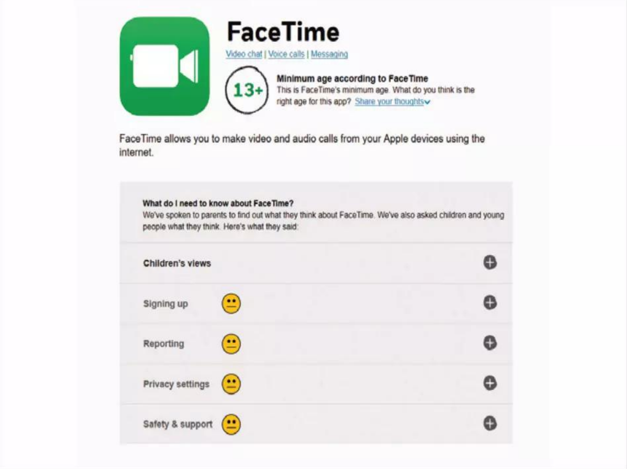
YouTube allows you to watch, create and comment on videos. You can create your own YouTube account, create a music playlist, and even create your own channel, which means you will have a public profile. YouTube allows live streaming.

What do I need to know about YouTube?
We've spoken to parents to find out what they think about YouTube. We've also asked children and young people what they think. Here's what they said:

Children's views ⊕
Signing up 😐 ⊕
Reporting 😐 ⊕
Privacy settings 😐 ⊕
Safety & support 😐 ⊕

FACETIME

Apple's FaceTime is one of the most used video chat clients available. However, it has been noted that people you don't know can FaceTime you and it's possible to record or take screen shots of a FaceTime conversation without you knowing.



FaceTime

Video chat | Voice calls | Messaging

13+ **Minimum age according to FaceTime**
This is FaceTime's minimum age. What do you think is the right age for this app? Share your thoughts

FaceTime allows you to make video and audio calls from your Apple devices using the internet.

What do I need to know about FaceTime?
We've spoken to parents to find out what they think about FaceTime. We've also asked children and young people what they think. Here's what they said:

Children's views ⊕
Signing up 😐 ⊕
Reporting 😐 ⊕
Privacy settings 😐 ⊕
Safety & support 😐 ⊕

Email & **Child**

We're often so concerned over social media, online gaming and chat sites that we tend to ignore one of the most common threats to online safety for young people and children, email. While it's a more manageable element, it does carry plenty of dangerous potential.

In reality it doesn't take too much of a technical genius to enter into a search engine, "fake email accounts" or something similar. The returned results, such as Fake Email Generator, Mailinator, ThrowAwayMail and FakeInbox are all designed to help you create a fake account that can either be single use or used regularly. This of course means that a person is able to create a false persona and sign up for Facebook and the like using a browser's private function, and have access to accounts without someone else knowing.

This works both ways, from the point of view of the young person gaining access to a site they shouldn't and for someone who's creating accounts ready for grooming, or something similar. With access to a fake email, a young person has the potential get into a variety of potential dangerous situations. They could be contacted by someone who is trying to groom or send radicalised content, they could also become the subject of a hack and unwittingly execute code that can deploy a virus, ransomware or other malware, along with possible backdoor hacks to gain access to the system the young person is using.

It's not just fake email sites that pose a danger when it comes to young people and children; although fake email sites usually don't have the better protection and anti-malware restrictions that more legitimate sites employ. Google Mail, Yahoo and so on can represent a weak link in the chain of digital protection for children and young people. The dangers are mostly the same but thankfully these online mail providers have better levels of malware protection.

So how would you, as a parent or guardian, combat potential email threats for children and young people? You may not be able to police their mobile accounts all the time but you can insist that they allow you access to the account on a regular basis to check that they're not in conversation with someone unknown, or that they're not receiving and responding to reams of spam and malware ridden emails. However, that does seem something of an Orwellian approach to managing a young person's email account.

Another possibility is to set up a family email account, separate from the parents or guardians' accounts, where the entire family has access and can utilise to sign up for games, safe sites and the like. It's a more open approach, whilst still preserving privacy for the adults and if you use folders within the email client or website, then there's some privacy for the young person too.

Naturally the best form of email attack and threat prevention is through education. Both the NSPCC and Childline recommend that you talk to your child and come up with a set of workable rules and conditions that are fair but protective. Educate them on the dangers of communicating with a stranger and inform them that online grooming takes place and how it works, also include how viruses work and other forms of malware, and how phishing and other forms of threats work too.

There are some tips that we as parents or guardians can use to help children and young people:

- Treat all people on the Internet as strangers, even those who could be friends.
- Never give out any personal information via email to an unknown source or site.
- Be wary when choosing an email name, don't use anything to identify your gender or anything provocative.
- Never open an email attachment. Check with a parent or guardian first.
- Never reply to an unknown email and never send any images of yourself.
- Always tell a parent, guardian or teacher if you've been contacted by someone you don't know.
- Never respond to a threating email or someone attempting to bait you into contact.
- Don't always believe everything you read in an email. Phishing attempts come as virus hoaxes.
- Don't believe you've won £1,000,000 or react to limited time ridiculous offers on technology or fashion. It's nearly always fake emails trying to get you to visit a site.

Another possibility is to use one of the many child friendly email programs and online services. There are ample available to try out and over the next couple of pages we take a look at ten of the more highly recommended services.

Email at first doesn't appear to be too much of a concern for the parent or guardian, after all we can view what emails are coming in to our accounts. However, it's not too difficult for a tech-savvy youngster to create an alternative email account, usually one that's web-based, that they can use to access games and sites you wouldn't normally allow them to.

> **"*Email Risks*"**

Safety

Top Child Friendly Email Programs and Services

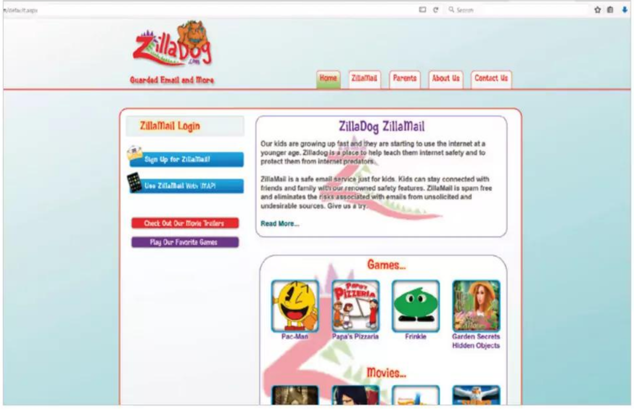
An email account for a child or young person is a great way for them to communicate with friends and family; however, as we've seen, it can be a dangerous tool. Therefore it's best to ensure they're using a safe, child friendly email account.

Ten Child Safe Email Accounts

It's not always easy to police and monitor an email account, so here are ten child friendly email accounts and related services that will help make the job of keeping children safer when communicating via email.

ZILLAMAIL

ZillaMail is run under the ZillaDog.com brand, created by parents for children. It's an easy to use, friendly service that also combines child safe online games and links to child safe websites, such as Cartoon Network and the like. ZillaMail has some interesting aspects and features, which makes it an excellent choice for parents and guardians.


ZillaDog
Guarded Email and More
Home
ZillaMail
Parents
About Us
Contact Us
ZillaMail Login
Sign Up for ZillaMail
Use ZillaMail With IMAP
Check Out Our Movie Trailers
Play Our Favorite Games
Games...
Pac-Man
Papa's Pizzaria
Frinkle
Garden Secrets Hidden Objects
Movies...

ZillaDog ZillaMail

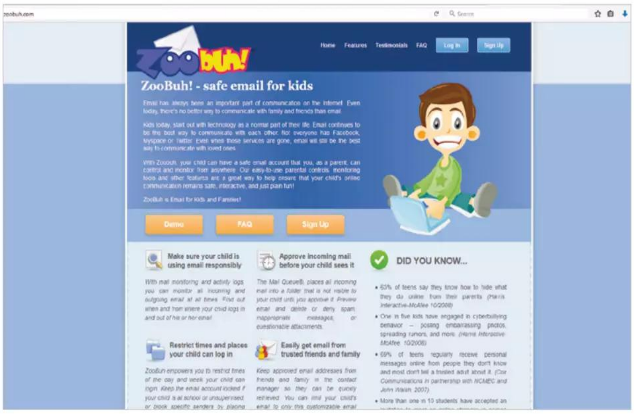
Our kids are growing up fast and they are starting to use the internet at a younger age. Zilladog is a place to help teach them internet safety and to protect them from internet predators.

ZillaMail is a safe email service just for kids. Kids can stay connected with friends and family with our renowned safety features. ZillaMail is spam free and eliminates the risks associated with emails from unsolicited and undesirable sources. Give us a try.

Read More...

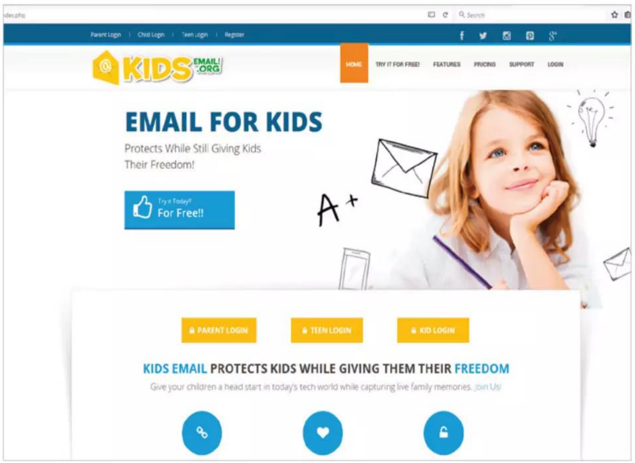
ZOOBUH

ZooBuh has an impressive list of benefits and features for parents and guardians to look over when considering an email provider for their child. Adjustable spam filtering, the ability to delete attachments, block specific senders, see activity logs and a Predator Catch Phrase alert system all add up to a great service.


zoobuh.com
Home
Features
Testimonials
FAQ
Log In
Sign Up
ZooBuh! - safe email for kids
Demo
FAQ
Sign Up
Make sure your child is using email responsibly
Approve incoming mail before your child sees it
DID YOU KNOW...
Restrict times and places your child can log in
Easily get email from trusted friends and family

KIDSEMAIL

KidsEmail is a paid for service, offering a 30 day free trial period. For your money you get mail monitoring for all incoming and outgoing emails from the child's account, time restrictions, blocked senders, no adverts, spam filtering and an easy way to add friends and family contact details.


Parent Login
Child Login
Teen Login
Register
KIDS EMAIL!.ORG
HOME
TRY IT FOR FREE!
FEATURES
PRICING
SUPPORT
LOGIN
Try it Today!
For Free!!
A+
PARENT LOGIN
TEEN LOGIN
KID LOGIN

EMAIL FOR KIDS

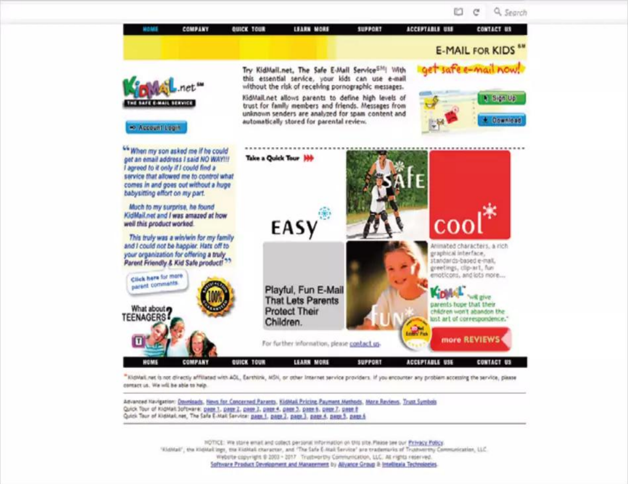
Protects While Still Giving Kids Their Freedom!

KIDS EMAIL PROTECTS KIDS WHILE GIVING THEM THEIR FREEDOM

Give your children a head start in today's tech world while capturing live family memories. Join Us!

KIDMAIL

KidMail is a low cost subscription email service that caters for both young children and older young people. Parents and guardians have full control over the email account and the messages that come and go from the child's account, along with many other benefits and features.


HOME
COMPANY
QUICK TOUR
LEARN MORE
SUPPORT
ACCEPTABLE USE
CONTACT US
E-MAIL FOR KIDS SM
KidMail.net SM
THE SAFE E-MAIL SERVICE
get safe e-mail now!
Sign Up
Download
Account Login
Take a Quick Tour
EASY
safe
cool
fun
What about TEENAGERS?
more REVIEWS
Click here for more parent comments

Try KidMail.net, The Safe E-Mail Service℠! With this essential service, your kids can use e-mail without the risk of receiving pornographic messages.

KidMail.net allows parents to define high levels of trust for family members and friends. Messages from unknown senders are analyzed for spam content and automatically stored for parental review.

"When my son asked me if he could get an email address I said NO WAY!!! I agreed to it only if I could find a service that allowed me to control what comes in and goes out without a huge babysitting effort on my part.

Much to my surprise, he found KidMail.net and I was amazed at how well this product worked.

This truly was a win/win for my family and I could not be happier. Hats off to your organization for offering a truly Parent Friendly & Kid Safe product!"

Playful, Fun E-Mail That Lets Parents Protect Their Children.

Animated characters, a rich graphical interface, standards-based e-mail, greetings, clip-art, fun emoticons, and lots more...

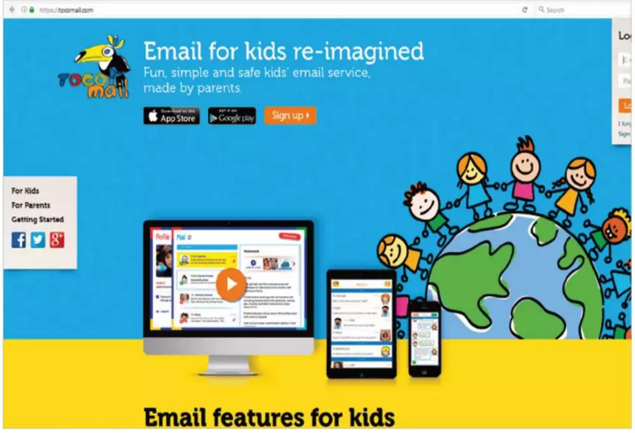
KidMail "will give parents hope that their children won't abandon the lost art of correspondence."

For further information, please contact us.

*KidMail.net is not directly affiliated with AOL, Earthlink, MSN, or other Internet service providers. If you encounter any problem accessing the service, please contact us. We will be able to help.

TOCOMAIL

Another well presented service, Tocomail offers the child, parent and guardian a wealth of fun and useful features. It brings a lot more than just email to the table, for example children get access to a drawing board app, to create their own attachments, whilst parents get notifications via an app when the child has received an email.


Email for kids re-imagined

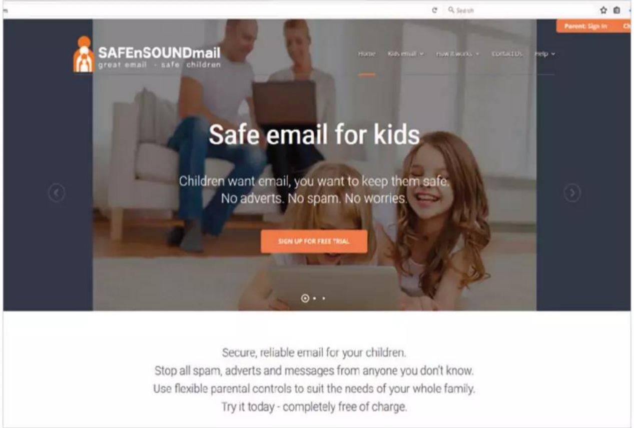
Fun, simple and safe kids' email service, made by parents.

Email features for kids

App Store
Google play
Sign up
For Kids
For Parents
Getting Started

SAFENSOUNDMAIL

SAFEnSOUNDmail has plenty of features available to those who purchase the subscription; however, there's a free 30-day trial to begin with. There's support for Apple, Android, Windows, Mac and Chromebook devices, up to five child accounts available, customisable controls and settings and elevated levels of encryption.


Safe email for kids

Children want email, you want to keep them safe. No adverts. No spam. No worries.

Secure, reliable email for your children.
Stop all spam, adverts and messages from anyone you don't know.
Use flexible parental controls to suit the needs of your whole family.
Try it today - completely free of charge.

SAFEnSOUNDmail
great email - safe children
SIGN UP FOR FREE TRIAL

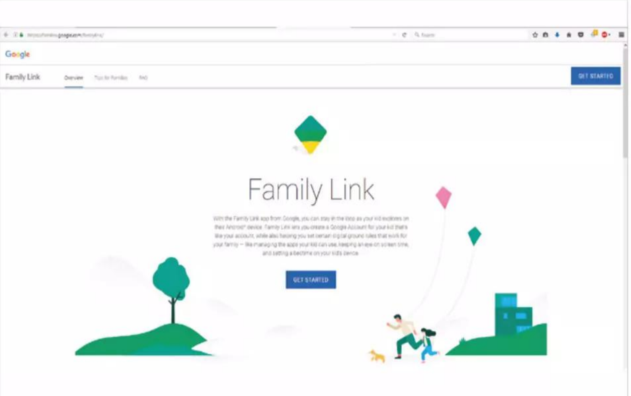
GMAIL

Providing your child is thirteen years or older, they can get access to a Gmail account. Gmail isn't the first email service that springs to mind when considering a young person friendly email account but with careful use of its filters, you can set up a good and reasonably safe email environment for them.

Gmail
TM
by Google

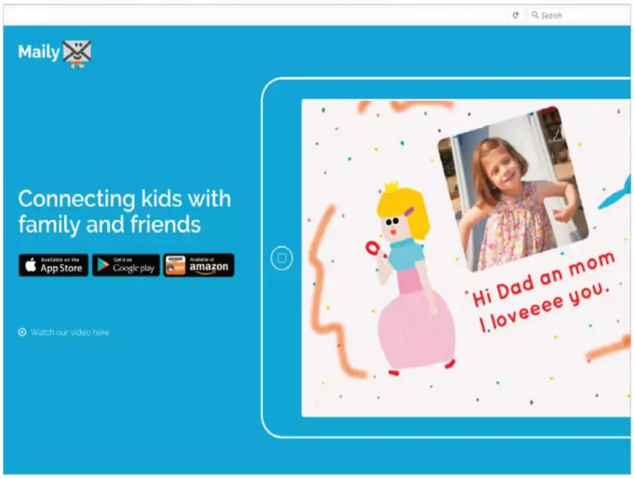
FAMILY LINK

Part of the services offered by Google, Family Link can help you set up a Gmail-like account for children under the age of thirteen. You need to be located in the US for the moment but the service offers improved controls for Android devices and apps and there are considerations for moving the service outside of the US in time.


Google
Family Link
Family Link
GET STARTED

MAILY

This is a child-friendly email app for iOS and Android devices. It's fun to use, secure and offers the parent or guardian ample control and restrictions for the child's account. With it children can stay in contact with specified contact lists, whilst still remaining safe online.


Connecting kids with family and friends

Maily
App Store
Google play
amazon
Watch our video here
Hi Dad an mom
I loveeee you.

SCHOOL EMAIL

Here's an interesting suggestion, why not use the child's school email? Providing the school is willing to participate, a child can log into their account from home and using the elevated security, send and receive emails in total safety. Naturally, you'd need to confirm with the school prior to using the email for personal contact.

Cyberbullying

Cyberbullying is when someone uses the Internet, email, online gaming, social media and any other kind of digital platform to threaten, tease, humiliate or upset someone else. Both the bully and the victim of the bullying can be any age, from very young children up to late teens, and beyond in some cases. The source of the bullying can come from others the victim knows at school or college, or from a complete stranger on the other side of the world.

Bullying someone online doesn't always involve threating remarks. What may seem like a playful comment on one side, could be taken as a cutting jibe on the other. It's not always an easy thing to specify, as we all have moments when we may say or do something to upset someone without meaning to do that person any emotional harm. Mostly though, with respect to a loose and throw-away comment, the one who made the comment will probably apologise for their mistake once they realise that they have upset the other person.

However, true cyberbullying is the persistent harassment of an individual. The cyberbully will goad, threaten, send nasty messages, even take images of the victim and Photoshop them in inappropriate situations, through the use of many different forms of online communications.

It's a sad case too, that a lot of young people are already in a heightened emotional state due to their body image, thanks to the media and unrealistic Photoshopping of celebrities. Where young people, especially young teens, are very conscious of their image, a slight remark to someone can impact the young person in an incredibly negative way.

Social Media

Probably one of the main platforms for cyberbullying, social media is an ideal hunting ground for the cyberbully. The effects of social media bullying have been devastating on some families. Teen suicides, self harm and elevated cases of depression amongst young people are popular in the media and bring to light just how powerful and dangerous social media is as a communications tool.

Facebook, Twitter, Instagram and other examples have all become the haunt of those who prey upon and harass others. From the point of view of a child, whose emotional state is quite vulnerable, even a simple 'like' of a comment can embarrass or hurt.

Online Gaming

Another prime source of modern cyberbullying, online gaming has proved to be a vicious place to inhabit for some. The problem with online gaming is that the bullying comes from anywhere in the world. There are cases of gamers targeting females, different religions or those who come from different parts of the world. With the use of headsets, the gaming cyberbullies are able to shout threats and taunt other gamers, rallying others around them until the victims feel overwhelmed by bullies.

There are numerous games which have adopted a more sport-friendly approach, introducing policies whereby instances of bulling can be reported and the bullies themselves have their gaming accounts suspended. Often online gaming bullying is just someone shouting 'noob' at another, degrading the victim as a newcomer, or someone who isn't as good as them. Other times the bully will say things like 'I hope you die' or 'I'm coming to kill you', or something similar. In short, any abusive behaviour, including destroying your online game creations or belongings, is a form of bullying.

Text Messaging

With more and more young people having access to their own phones or tablets, abusive text messaging is becoming a major issue. Messages sent can, thankfully, be easily traced back to the source, and together with anyone else who was involved, the bully(s) can be reprimanded for their behaviour. Sadly though, there are ways to hide texts and with such knowledge, a cyberbully is able to send their abusive texts anonymously.

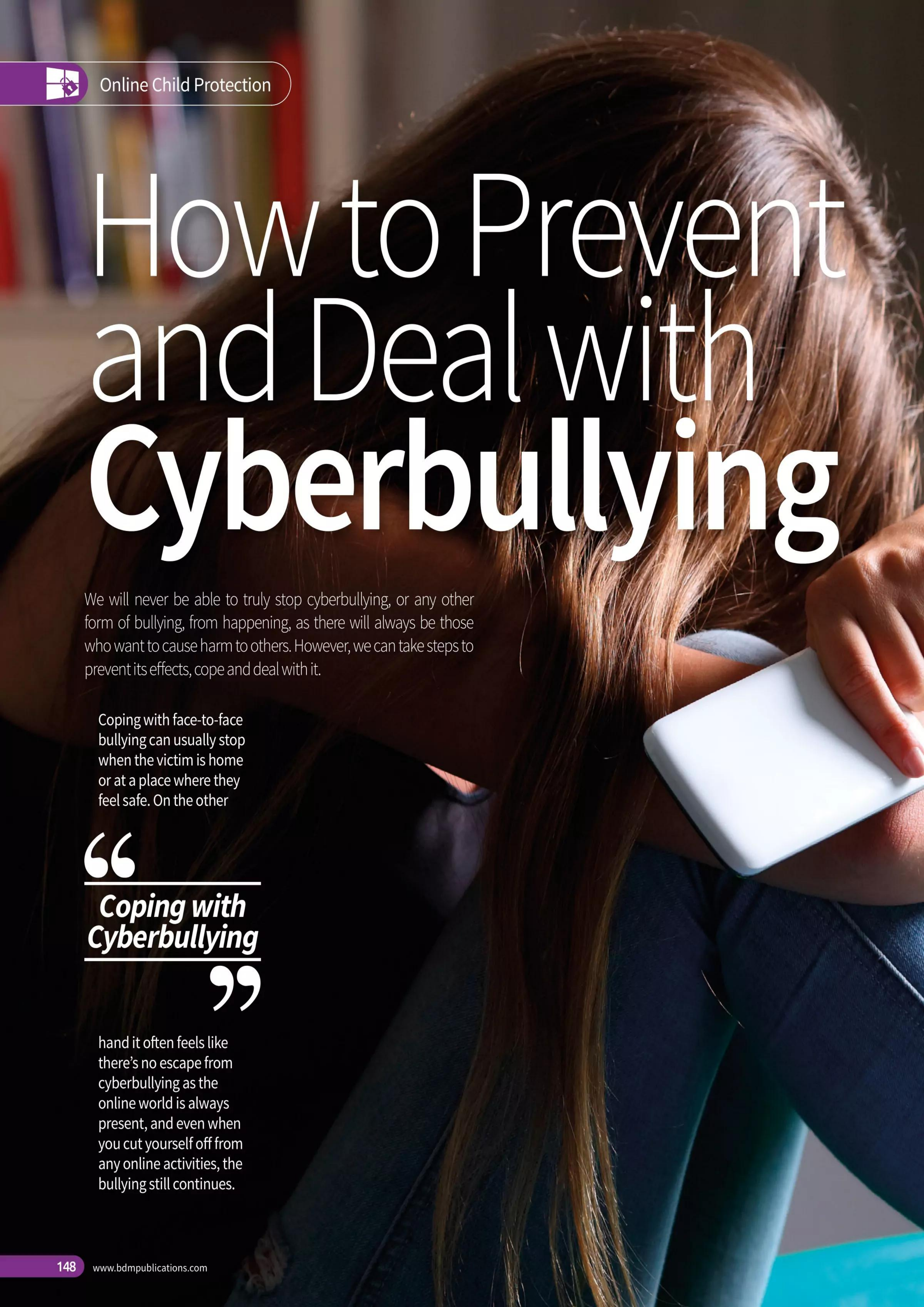
Another aspect of cyberbullying via text message is sexting. This is when someone takes an explicit image or video of themselves and sends it to someone else. Sometimes, a person can bully someone into sending them images or videos of the victim, then send those images on to others or upload them to popular sites and inform an entire group of their location.

Email

Sending abusive emails is a large area of concern for those involved in protecting young people from cyberbullying. We've seen, the double-edged blade of anonymity can cut both ways: it can protect your identity online but it also hide an individual who is bullying someone. Anonymous emails sent from a bully can be just as harmful as social media, online gaming and texting. It's a more personal form of bullying, much like having an abusive letter addressed and posted directly to you.

Setting up filters to block certain senders does work but only to a small degree. There are plenty of email services available that will hide a sender or fake email providers to hide behind. It's not always abusive content either, as cyberbullies have been known to send viruses and other malware via email to their victims.

Cyberbullying covers many different forms and platforms. It can be a single, throw-away comment, a like on a Facebook comment or just someone calling someone else a 'noob'. It can also be very serious indeed, including death threats, threats of violence or the sending or posting of explicit images or videos. There's a wealth of information available from the likes of the NSPCC and Childline with regards to cyberbullying, which is certainly worth reading through if you suspect any instances of bullying or you just want to know more about how it works online.



How to Prevent and Deal with Cyberbullying

We will never be able to truly stop cyberbullying, or any other form of bullying, from happening, as there will always be those who want to cause harm to others. However, we can take steps to prevent its effects, cope and deal with it.

Coping with face-to-face bullying can usually stop when the victim is home or at a place where they feel safe. On the other hand it often feels like there's no escape from cyberbullying as the online world is always present, and even when you cut yourself off from any online activities, the bullying still continues.

> **"Coping with Cyberbullying"**

The level of how upset a victim of cyberbullying feels depends greatly on the person. Some can easily shake it off or deal with it by immersing themselves in a sport, book, family or something else. Others though, take any form of abusive message, comment and such to heart and its affects can range from crying to feeling suicidal. There's a lot that goes on in between and it's difficult even for professionals and experts to say how to react and cope with cyberbullying.

However, there are some guidelines which we can help children and young people through when it comes to dealing with cyberbullying:

It's not your fault – If someone is repeatedly cruel to you, you must not blame yourself. Two people can have an argument but if the other person continually abuses you in some form, then that's bullying and is not acceptable.

Don't respond – No matter how easy or tempting it is to respond to a cyberbully, it's recommended that the young person doesn't. Often, a cyberbully is goading the victim for a response, it's a form of psychology that enables them to think they have power over the victim.

Save all evidence – It's important that the young person saves or records all the evidence of cyberbullying. This evidence can then be used to show a parent or guardian, teacher or relative, or even someone responsible for the platform where the bullying took place. This way action can be taken to prevent any escalation.

Always ask for help – Even if the bullying incident seems minor, such as a throw-away comment, it's always best for the young person involved to tell their parent or guardian. We, as adults, can then help the young person deal with the bullying.

Measure your response – It's very easy as a parent or guardian to make a knee-jerk reaction to someone who's cyberbullying our child. Therefore it's often best to take evidence, then perhaps contact someone else, such as the NSPCC or local councillor to see what they as professionals recommend as a gauged response.

Take time to listen – A young person coming to an adult for help on bullying is a huge step for them. It's easy to close up as a child, so to take that step should be worthy of your full attention. Listen to everything they have to say and together find a way to prevent and deal with the cyberbullies.

Help restore self-respect – The ultimate goal in any bullying is help restore self-respect to the victim. The more self-respect the young person has, then the better they are able to cope with future bullies, and life itself.

Stay positive – Bullying should be stopped but it's unlikely as humans will never be able to eradicate all forms of cruelty toward others. With that in mind, it's best to remain positive for the young person, whilst still being realistic. It will help them mature and learn to form protection techniques against those who want to cause suffering.

Ask the person to stop – Whilst one of the guidelines is to never respond, there is the option to take a simple approach and ask the person who's bullying to stop. Sometimes a hurtful comment could be easily rectified by the sender, simply by it being shown that it was unnecessarily cruel. In the ideal world, they will apologise and remove the comment. It depends greatly on the comment and bullying in question.

Use the tools available – Use the available filters, blocks and reporting mechanisms available to stop the cyberbully from even being able to contact you. Facebook, Twitter and so on can block users and you're able to report abusive behaviour. Likewise, online gaming can ban an account or kick a bully from the game server.

Report serious threats – Not only should you report threats to parents and guardians, it's recommended that you should report serious physical, sexual and violent threats to the police. Each case will be treated with respect and the police have powers to approach the bully with the evidence to caution or charge.

Whilst the above will help children, young people, parents and guardians with cyberbullying, it's sadly not something that's going to disappear overnight. The moment you're online, you're open to some form of abusive behaviour and every social media, online game and contact made increases the chances of cyberbullying from occurring. The best we can do is help young people cope with it and learn to avoid those who would want to abuse.

Helping Your Child Through the Internet

The Internet is a vast resource that's full of amazing details and an equal amount of villainy and inappropriate content. It's difficult for a child to navigate it by themselves and extremely dangerous; so, as a parent or guardian, we need to make sure they're safe.

Internet Safety for Everyone

Together with the excellent advice from the NSPCC, Childline and Safety Net Kids, we've collated ten practical and realistic tips to help you and your child remain safe when using the Internet and its connected services.

PERSONAL INFORMATION

Never post any personal information online. Keep your postal address, email address, phone numbers and, if possible, names away from public viewing. Especially never tell anyone you've just met online, in a game or chat room any details about yourself.

PERSONAL INFOR
Mr.
Mrs.
Ms.
First Name
Last Name

PHOTOGRAPHS

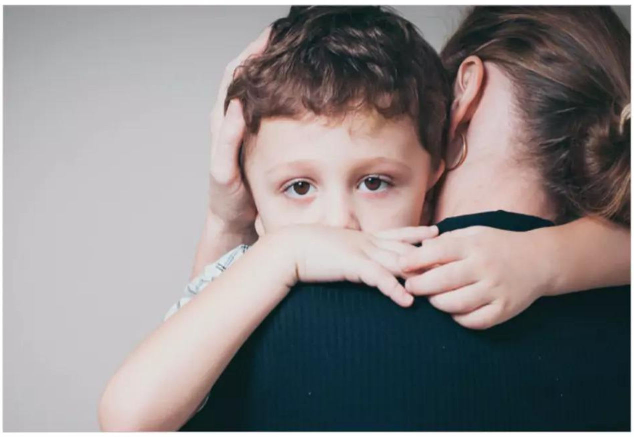
Consider carefully before posting any pictures of yourself online. Once an image is available on the Internet, it's extremely difficult to get rid of any trace of it; and should someone have already downloaded it on to their computer, it's impossible to locate and trace.

STRANGER DANGER

People you don't know in the real world are strangers and not always who they say they are. The same applies for the online world. Not everyone you meet in an online game is who they claim to be, so treat every contact as a stranger and be wary of them.

INAPPROPRIATE CONTENT

If you see or hear something online that upsets you or makes you feel uncomfortable, you must tell a parent, guardian or teacher as soon as you can. If possible, show them the content that's upset you and tell them why it's upsetting. Talking to a parent or teacher will help you gain a better understanding of the world around you.

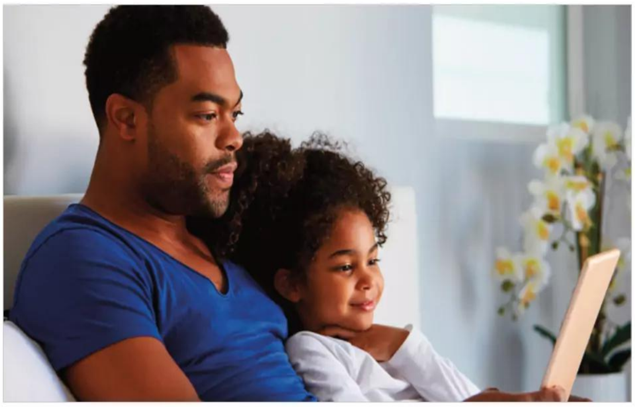


COMMENTS

Always think before you enter any comments online. Remember, they can be hurtful to someone else or be inappropriate without you even realising it. The comments could also lead someone to taking an interest in you, if you enter your age for example.

ACCOMPANIED VIEWING

Parents, always make sure that young children are accompanied when navigating the Internet. Ensure that the privacy and security settings are as high as possible and that they don't have access to sites beyond what you specify, should you need to leave their side for a moment.

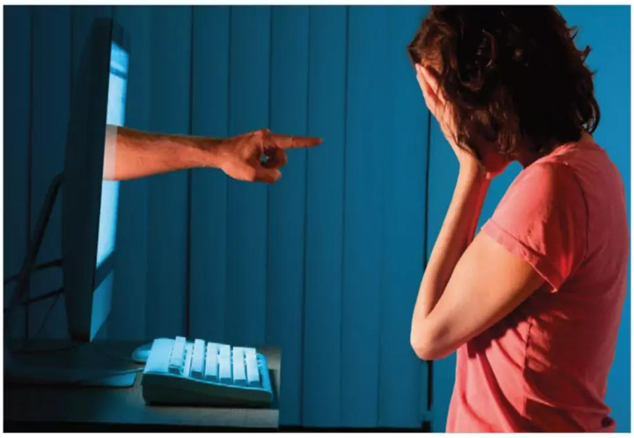


SECURE PASSWORD

Never give out your password online, even if the email or message is claiming to be from the bank or someone you know. Never let anyone remotely attach to your computer either. It's very rare for a company to attach to a home computer to fix something. At least be suspicious of anyone asking to connect remotely.

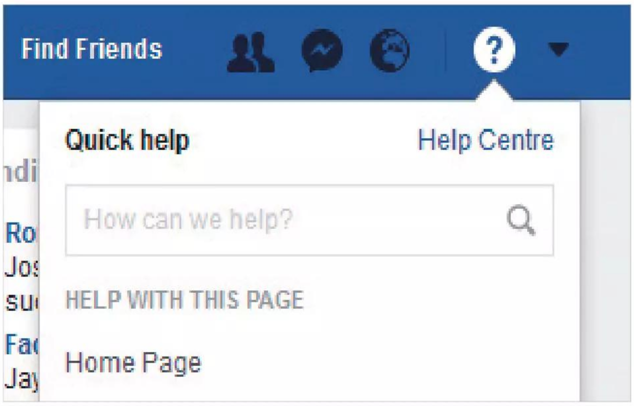
IGNORE BULLYING

Try not to reply to anyone who's appearing to bully you online. They are most likely trying to goad you into responding and will keep pushing until you finally crack and respond. Most of all, never respond out of anger. If it's getting too much, leave the site or game and come back later.



SOCIAL SAFETY

Whether you're on a social media site, in a chat room or playing a game, become familiar with the safety settings: how to turn off chat and how to block or report another user for any abusive content they may post. Take screenshots if possible, so you have evidence to back up your claim.



NEVER MEET

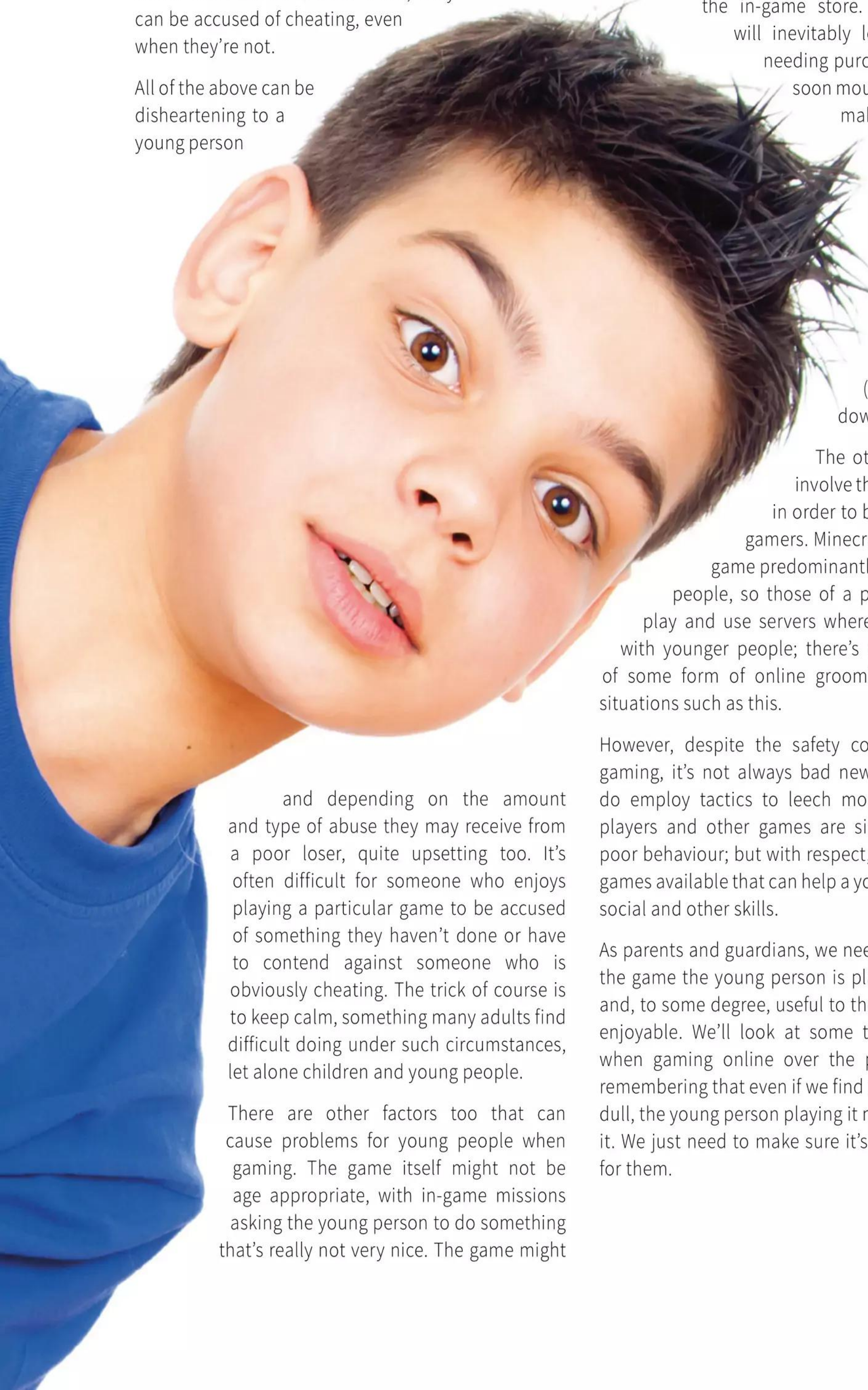
Never arrange to meet up with anyone you've met online, even if you're an older teenager. It's very easy to pretend to be someone, post a fake picture or take the identity of someone else. If you do arrange a meeting, make sure you're with other friends, in a public place and let others know where you are going.

Your Child and Online Gaming, is it Safe?

Gaming has taken some interesting leaps in technology since the days of feeding money into the arcade cabinets. However, with those advances comes a new level of online concerns for parents and guardians.

Of course, there's nothing wrong with gaming or online gaming. Despite the many years of people bemoaning that gaming is taking away something from a childhood, recent studies have actually shown that online gaming can increase social skills, help develop hand-to-eye coordination and, depending on the game, have educational benefits and help young people learn.

The problem is that not everyone always plays fair; some take great offence when they've been beaten by another player, resulting in the person beaten shouting or entering abusive comments. Other players use cheats to gain an advantage, making it near impossible for other players to even have a chance of winning or succeeding. Sometimes, when a player is better than others around them, they can be accused of cheating, even when they're not.



All of the above can be disheartening to a young person and depending on the amount and type of abuse they may receive from a poor loser, quite upsetting too. It's often difficult for someone who enjoys playing a particular game to be accused of something they haven't done or have to contend against someone who is obviously cheating. The trick of course is to keep calm, something many adults find difficult doing under such circumstances, let alone children and young people.

There are other factors too that can cause problems for young people when gaming. The game itself might not be age appropriate, with in-game missions asking the young person to do something that's really not very nice. The game might involve some scenes of an inappropriate nature, perhaps sexually explicit or extremely violent, or use inappropriate language.

In terms of online bullying, it's not just rage that causes problems. Griefing is a tactic used by some gamers to bully others into making the wrong move or decision in the game. This way, the 'griefer' wins by simply causing as much aggravation as possible, and in turn enrages those around them. It's also not unheard of for entire teams of griefers to band together to bully the opposition into defeat.

In-game spending is a modern cause for concern among parents too. For the young person who enjoys playing the game to have any significant advantage at all, they may need to purchase better items from the in-game store. Often these items will inevitably lead to more items needing purchasing and the cost soon mounts up. Other games make it near impossible to finish without having to pay for something, such as a key to unlock the next level or by having the player buy and download more content (known as a DLC, downloadable content).

The other safety concerns involve those who play games in order to be exposed to young gamers. Minecraft, for example, is a game predominantly played by younger people, so those of a perverse nature may play and use servers where they're interacting with younger people; there's even the possibility of some form of online grooming taking place in situations such as this.

However, despite the safety concerns over online gaming, it's not always bad news. Yes some games do employ tactics to leech more money from the players and other games are simply an excuse for poor behaviour; but with respect, there are countless games available that can help a young person develop social and other skills.

As parents and guardians, we need to make sure that the game the young person is playing is appropriate and, to some degree, useful to them, as well as being enjoyable. We'll look at some tips on staying safe when gaming online over the page but it's worth remembering that even if we find the game somewhat dull, the young person playing it may well be enjoying it. We just need to make sure it's a safe environment for them.

Online is playing a game in real time with other players from around the world. The game can be virtually anything, a shooter, role playing, adventure or something open world, such as Minecraft. The issue with online gaming is that anyone could be the character that's currently playing next to your child's online avatar.

> **“Online Gaming”**

Staying Safe when Gaming Online – Advice for Your Child

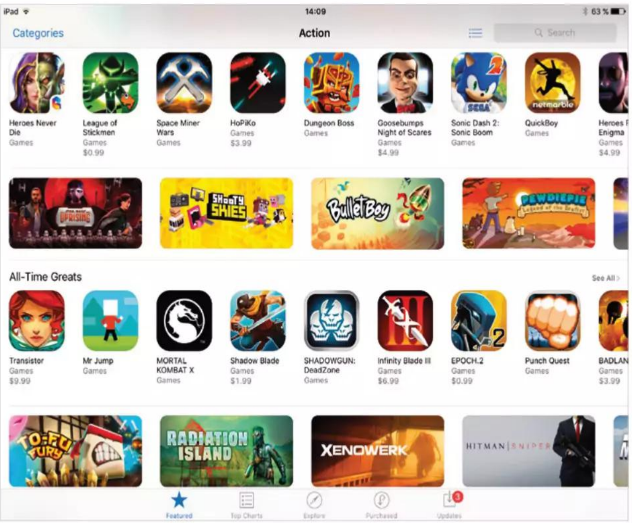
We've looked at the safety concerns of online gaming but what can we as parents and guardians do to help keep our young gamers safe? Thankfully, it's nothing too drastic, just a little common sense and a few tips to help out.

Game On

Here are ten tips to help the young gamer get the best from their game of choice, whilst still remaining safe; also how to avoid any conflicts that may arise from the gaming community.

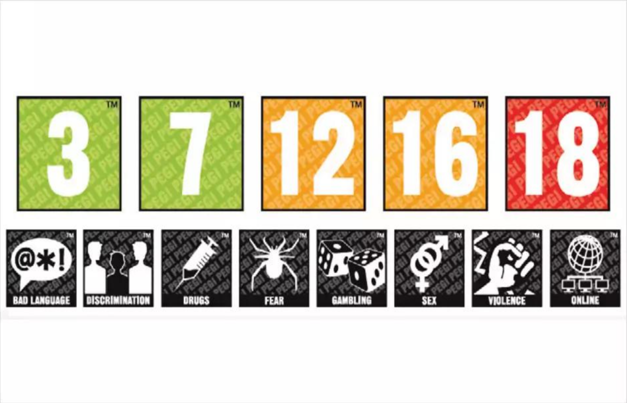
INVOLVED PARENTS

Parents, take an interest in the online games that your child plays. See what type of game it is and especially see what the online community is like. View the in-game chat, and read the game's forum if it has one to gauge the type of gamers who play it.


iPad
14:09
63 %
Categories
Action
Search
Heroes Never Die
Games
League of Stickmen
Games
$0.99
Space Miner Wars
Games
HoPiKo
Games
$3.99
Dungeon Boss
Games
Goosebumps Night of Scares
Games
$4.99
Sonic Dash 2: Sonic Boom
Games
QuickBoy
Games
Heroes Enigma
Games
$4.99
UPRISING
SHOOTY SKIES
Bullet Boy
PEWDIEPIE
All-Time Greats
See All
Transistor
Games
$9.99
Mr Jump
Games
MORTAL KOMBAT X
Games
Shadow Blade
Games
$1.99
SHADOWGUN: DeadZone
Games
Infinity Blade III
Games
$6.99
EPOCH.2
Games
$0.99
Punch Quest
Games
BADLAND
Games
$3.99
TO-FU FURY
RADIATION ISLAND
XENOWERK
HITMAN | SNIPER
Featured
Top Charts
Explore
Purchased
Updates

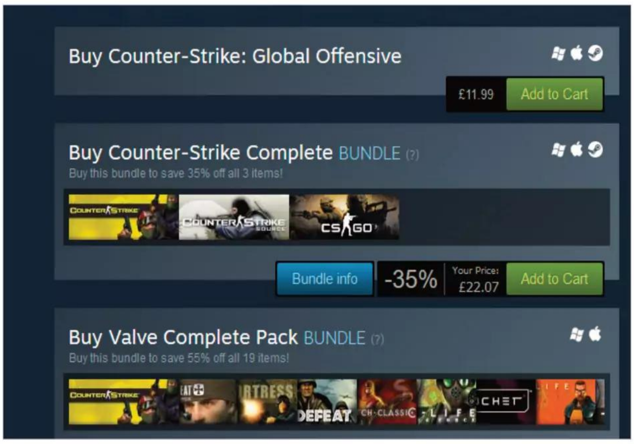
AGE APPROPRIATE

Make sure that game you're playing is age appropriate. Whilst it's fun being nine and playing an 18-rated game, there's bound to be content within that may upset or offend you. There's a reason certain types of game have an age restriction.


3
7
12
16
18
BAD LANGUAGE
DISCRIMINATION
DRUGS
FEAR
GAMBLING
SEX
VIOLENCE
ONLINE

IN-GAME SPENDING

However tempting it is to buy an on-game item or DLC, it's not always the best idea. Items like this can be a lure for you to buy another and another, until the cost mounts up and you've racked up a game bill in the hundreds. If you desperately need an item, discuss it with a parent or guardian.



Buy Counter-Strike: Global Offensive

£11.99 Add to Cart

Buy Counter-Strike Complete BUNDLE (?)

Buy this bundle to save 35% off all 3 items!

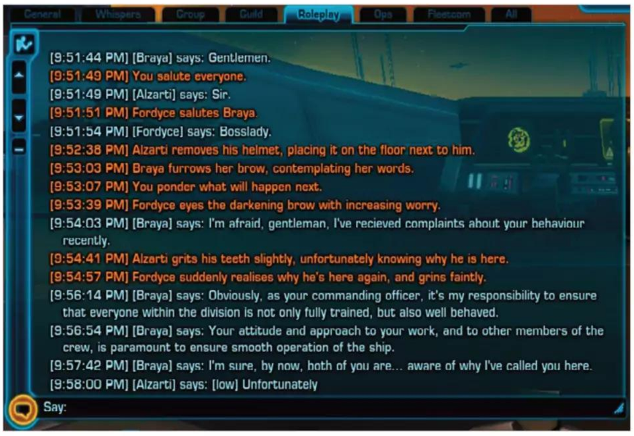
Bundle info -35% Your Price: £22.07 Add to Cart

Buy Valve Complete Pack BUNDLE (?)

Buy this bundle to save 55% off all 19 items!

CAREFUL CHATTING

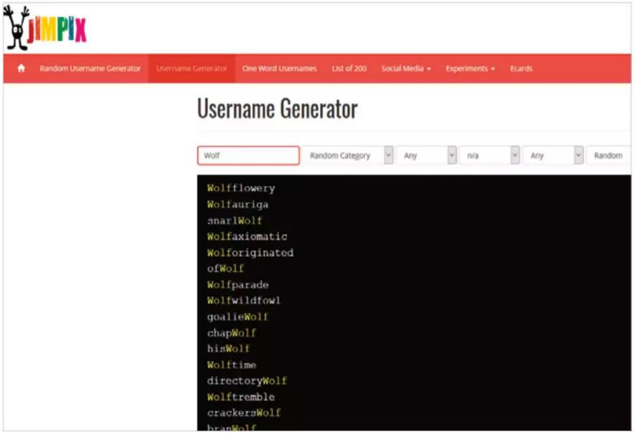
Not everyone in the game is going to be the same age as you. There are some people who are much older and who like to pretend they're a young person. Don't be fooled into becoming a friend with someone who's playing with you. Enjoy the game, and playing with others, but don't arrange any out of game communications.


General
Whispers
Group
Guild
Roleplay
Ops
Fleetcom
All
Say:

```
[9:51:44 PM] [Braya] says: Gentlemen.
[9:51:49 PM] You salute everyone.
[9:51:49 PM] [Alzarti] says: Sir.
[9:51:51 PM] Fordyce salutes Braya.
[9:51:54 PM] [Fordyce] says: Bosslady.
[9:52:38 PM] Alzarti removes his helmet, placing it on the floor next to him.
[9:53:03 PM] Braya furrows her brow, contemplating her words.
[9:53:07 PM] You ponder what will happen next.
[9:53:39 PM] Fordyce eyes the darkening brow with increasing worry.
[9:54:03 PM] [Braya] says: I'm afraid, gentleman, I've recieved complaints about your behaviour
   recently.
[9:54:41 PM] Alzarti grits his teeth slightly, unfortunately knowing why he is here.
[9:54:57 PM] Fordyce suddenly realises why he's here again, and grins faintly.
[9:56:14 PM] [Braya] says: Obviously, as your commanding officer, it's my responsibility to ensure
   that everyone within the division is not only fully trained, but also well behaved.
[9:56:54 PM] [Braya] says: Your attitude and approach to your work, and to other members of the
   crew, is paramount to ensure smooth operation of the ship.
[9:57:42 PM] [Braya] says: I'm sure, by now, both of you are... aware of why I've called you here.
[9:58:00 PM] [Alzarti] says: [low] Unfortunately
```

NOTHING PERSONAL

Never give out any personal details into an in-game chat window, via your headset or in a game's forum. These places are ideal hunting grounds for those who want to use that information to their advantage. Make sure your username isn't linked to you in real life too.


JIMPIX
Random Username Generator
Username Generator
One Word Usernames
List of 200
Social Media
Experiments
Ecards

Username Generator

Wolf | Random Category | Any | n/a | Any | Random

```
Wolfflowery
Wolfauriga
snarlWolf
Wolfaxiomatic
Wolforiginated
ofWolf
Wolfparade
Wolfwildfowl
goalieWolf
chapWolf
hisWolf
Wolftime
directoryWolf
Wolftremble
crackersWolf
branWolf
```

NO GRIEVING

Try not to get angry or be fooled by someone who's being nasty in the game. They could be baiting you, griefing you into making a mistake or simply just a cyberbully who's looking for someone new to inflict misery on. Don't react to anyone calling you a noob, loser or any such wording.

STOP GRIEFING!

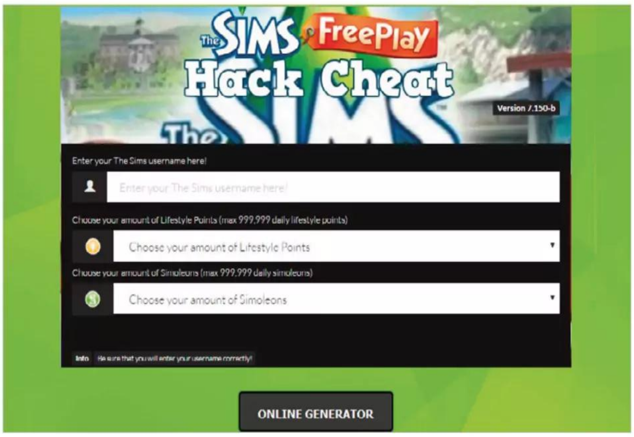
AVOID CHEATING

Cheats are everywhere. Even in the most secure game, there will be a time when someone releases a cheat code that can grant them immortality, infinite items or something else that enables them to win all the time. If you can, record their activity and report them to the game server admins.

If At First You Don't Succeed
↑↑↓↓←→←→ B A
Try Try Again

AVOID HACKING

Don't attempt to download or sign up for a site that claims to give you an in-game advantage or cheat. Some downloads and sites contain malware payloads or are trying to scam you in some way. Whilst it's tempting to have the advantage, it's nearly always some form of phishing scam.


The SIMS FreePlay
Hack Cheat
Version 7.150-b
ONLINE GENERATOR

Enter your The Sims username here!

Enter your The Sims username here!

Choose your amount of Lifestyle Points (max 999.999 daily lifestyle points)

Choose your amount of Lifestyle Points

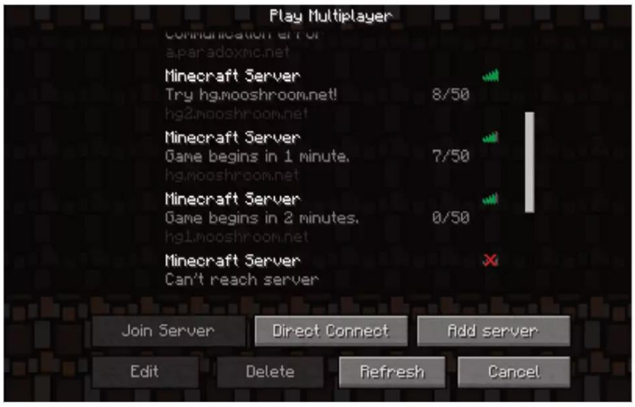
Choose your amount of Simoleons (max 999.999 daily simoleons)

Choose your amount of Simoleons

Info He sure that you will enter your username correctly!

ALTERNATIVE SERVERS

If you find yourself on a server with cheats, the subject of griefing or other forms of bullying, then leave the server and see if there's another one available without these people present. It might also just be a bad time of day, so try again later on.


Play Multiplayer
Join Server
Direct Connect
Add server
Edit
Delete
Refresh
Cancel

Communication error
a.paradoxmc.net

Minecraft Server
Try hg.mooshroom.net! 8/50
hg2.mooshroom.net

Minecraft Server
Game begins in 1 minute. 7/50
hg.mooshroom.net

Minecraft Server
Game begins in 2 minutes. 0/50
hg1.mooshroom.net

Minecraft Server
Can't reach server

WARY TRADING

Be wary of any in-game comments offering a discount on in-game items or trades. Whilst some are legitimate, people wanting to trade one item for another, others are trying to scam you out of real money or in-game cash or items.

MATCHMAKING: SOLO
SATURN
URANUS
NEPTUNE
PLUTO
CERES
SEDNA
MERCURY
Recruiting
Trading
-DarkTenno-
-V-E-G-A-
21stgun-EN-
_AzE_BoSS_
Rue
yogoy
AHRI3
ALIAS2050
ArchonLegend
HOLD RIGHT CLICK TO ROTATE

Monitoring What's Going On

The temptation and lure of the Internet is often a little too much for some people, especially young people who are repeatedly told not to look or go somewhere on it. Tell a young person not to open a box and most will lift the lid when you're not around.

The tech-savvy youngsters of today will already have a better idea of how to circumvent technological restrictions that we've put in place. We're not saying they're hacking or do anything particularly bad, it's just that sometimes we need to see what all the fuss is about ourselves, rather than take someone else's word for it. Here then, are some of the tricks that the modern, digitally capable young person can do to hide what they look at on the Internet.

Private Browsing

Private browsing, privacy mode or incognito mode is a feature built into every browser, regardless of the computer or device's operating system. It is, as the title suggests, a privacy feature that will disable the browsing history and web cache; it stops any data from the browsing activities from being stored on the device or computer.

With private browsing mode enabled, which takes just a couple of clicks of the mouse, someone can effectively run a search for something they shouldn't, view the content and close down the private browser window without anyone ever knowing they were on the site. There are ways and means in which you can check for private browsing but it's often hit and miss and not entirely accurate, which is the whole point of private browsing in the first place.

Webmail

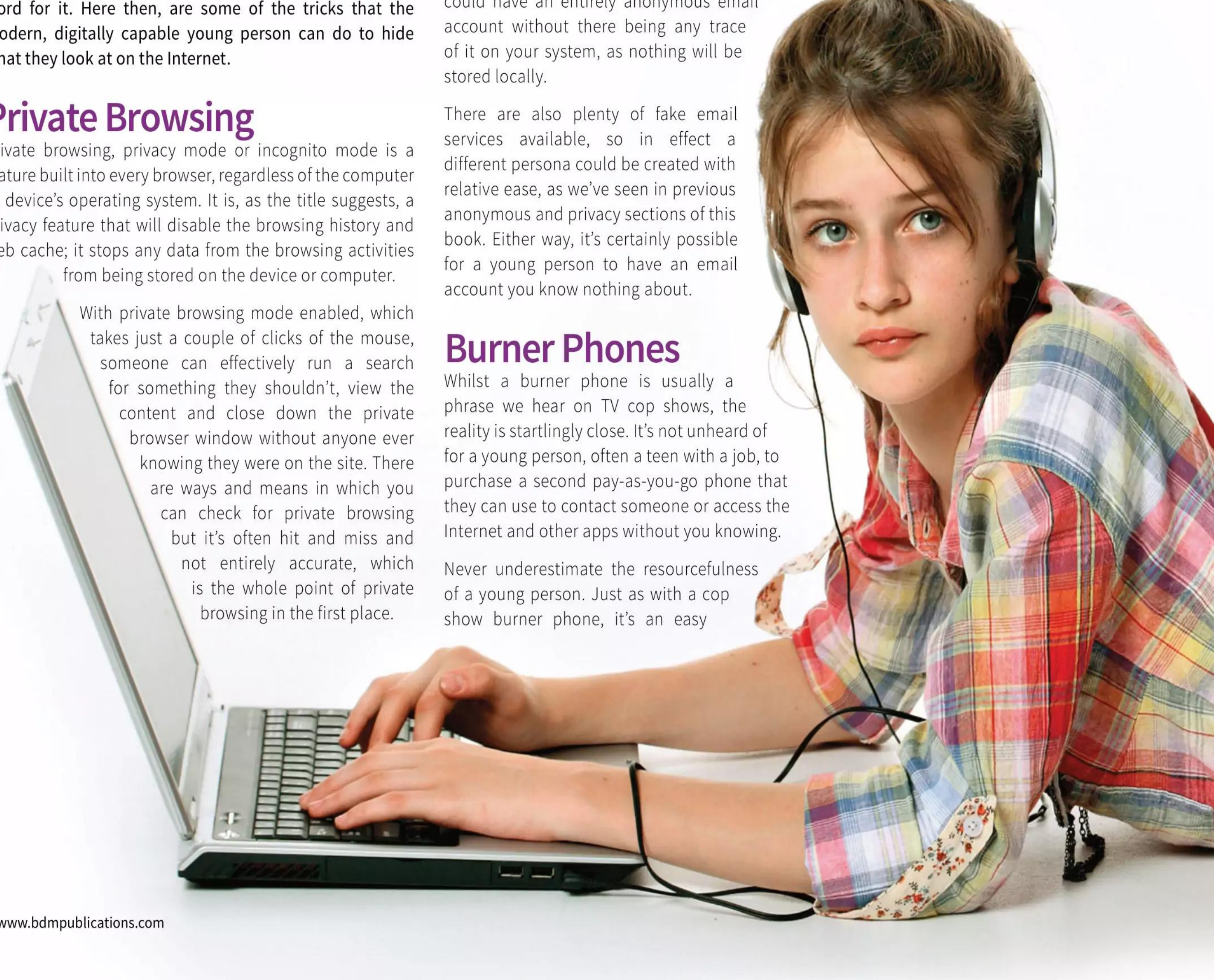
It's easy enough for someone to create a webmail account, such as Yahoo or Gmail and use it without anyone knowing of its existence. Combine a webmail account with private browsing, for example, and a young person could have an entirely anonymous email account without there being any trace of it on your system, as nothing will be stored locally.

There are also plenty of fake email services available, so in effect a different persona could be created with relative ease, as we've seen in previous anonymous and privacy sections of this book. Either way, it's certainly possible for a young person to have an email account you know nothing about.

Burner Phones

Whilst a burner phone is usually a phrase we hear on TV cop shows, the reality is startlingly close. It's not unheard of for a young person, often a teen with a job, to purchase a second pay-as-you-go phone that they can use to contact someone or access the Internet and other apps without you knowing.

Never underestimate the resourcefulness of a young person. Just as with a cop show burner phone, it's an easy



enough device to hide from a parent or guardian. Naturally there's a limit to what a young person can get away with but it's something worth keeping in mind. Another of the many elements to look out for with a young person who's being groomed, is a burner phone the groomer may give to them. This way, they're able to contact the young person with a higher degree of anonymity.

Secret Social Media

When used with an unknown webmail address, and private browsing, it's an easy task to create a secret social media account. Try it yourself and see how far you can get using Twitter and Facebook and the like.

Despite the fact that creating a fake social media account is against the social media platform's rules, it's not something they're able to police with any great efficiency. Just like a secret email, it's extremely difficult to see if a young person has set up a secret social media account.

OS on a stick

It's possible to have an entire operating system on a USB stick and be able to boot into the OS outside the system that's installed on the computer. This makes for an impressively anonymous and secure platform to browse from, as everything is done via the USB stick and the temporary session held in memory.

Naturally, the young person will need to reboot the computer and boot into the OS on the USB drive but that takes mere seconds these days. The end result is something you'll never likely be aware of.

Of course, we're not saying you should police your children like a prison warden. There will come a point where you simply have to have faith that you've taught them right from wrong and let them go and discover the world by themselves, however painful that may be. There's a fine line between protection and controlling and its borders are ever shifting thanks to the technology available and the ever-growing curiosity of young people.

However, we can make sure that a young person is educated and Internet-wise enough to be able to make decisions for themselves; and, as you would expect, we also need to ensure that they're not the victim of any digital attack. An open relationship is credited as being the key here, as often stated by professional bodies.

Eyes in the Back of Your Head

Human nature finds most of us sneaking a peek at something we shouldn't and children and young people are certainly no different. Young children will most likely avoid those areas on the Internet the parent or guardian has told them to never go to; however, older children and teens may find it a little too tempting.

Monitoring Online Activity for Non-Technical Guardians

There's a vast difference between monitoring a child's online activity and actively spying on everything they do. In monitoring, you're making sure that they aren't being scammed, downloading anything illegal and generally behaving themselves online.

Non-Technical Tips for Monitoring

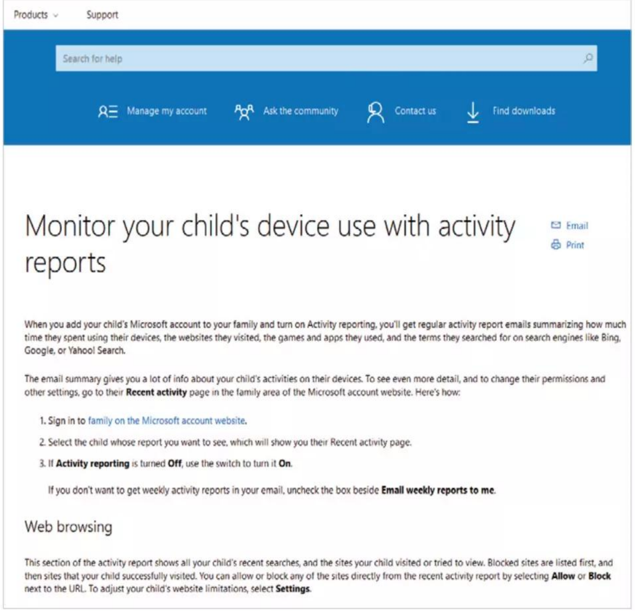
There are numerous ways to monitor a child's online safety but a lot of them can be quite technical. Instead, here are ten tips for those who aren't as computer literate but still want to help keep a child safe online.

DEFINE RULES

First off, set some rules. Don't use the Internet alone in your room, don't chat with anyone online, don't enter your full name or address online, don't click on any links, don't open any attachments, and talk if you see something that's upsetting. Common sense rules will go a long way to ensuring online safety.

FAMILY ACCOUNTS

Consider using the Microsoft Family Account as your child's login to Windows 10. We'll go into more detail as how to set it up and use it a bit later on. For now though, navigate to **https://support.microsoft.com/en-us/help/12441/microsoft-account-monitor-child-device-activity** and see what you can do with a child account in Windows 10.



Monitor your child's device use with activity reports

When you add your child's Microsoft account to your family and turn on Activity reporting, you'll get regular activity report emails summarizing how much time they spent using their devices, the websites they visited, the games and apps they used, and the terms they searched for on search engines like Bing, Google, or Yahoo! Search.

The email summary gives you a lot of info about your child's activities on their devices. To see even more detail, and to change their permissions and other settings, go to their **Recent activity** page in the family area of the Microsoft account website. Here's how:

1. Sign in to family on the Microsoft account website.
2. Select the child whose report you want to see, which will show you their Recent activity page.
3. If **Activity reporting** is turned **Off**, use the switch to turn it **On**.

If you don't want to get weekly activity reports in your email, uncheck the box beside **Email weekly reports to me**.

Web browsing

This section of the activity report shows all your child's recent searches, and the sites your child visited or tried to view. Blocked sites are listed first, and then sites that your child successfully visited. You can allow or block any of the sites directly from the recent activity report by selecting **Allow** or **Block** next to the URL. To adjust your child's website limitations, select **Settings**.

ISP HELP

If you require some extra help with monitoring the Internet activity in your home, consider contacting your ISP and chatting with a member of the team. Most, if not all, ISPs will have a dedicated section for online safety, in particular child safety and may be able to set up a web-based monitoring portal for you.

ISP
Internet Service Provider

BE PRESENT

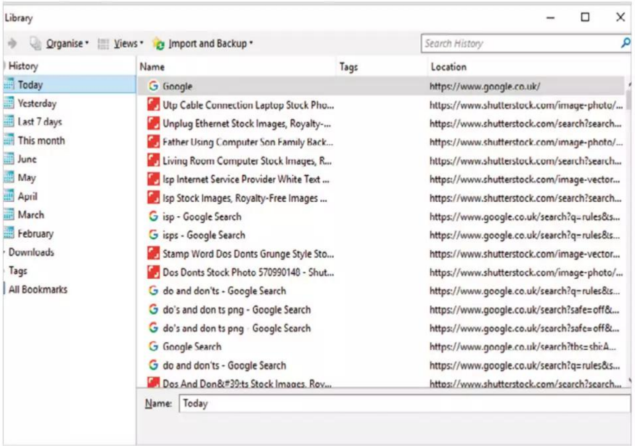
Even if there are multiple computers and devices in the home, only allow the child to use one located in a main living area, such as the living room. Somewhere you're likely to be when they're online, so you can keep an eye on them and be at hand if they come across anything.

GOING OFFLINE

If your child wants to play a game, one that doesn't involve any online communications, or do some work, consider unplugging the computer or device from the home router. Either pull the cable out of the network port or power down the Wi-Fi. That way they can't get online.

BROWSER HISTORY

After your child has been online, consider taking a look at the browser history. You can find the history among the browser's usual settings, click on the three horizontal bars in the top right of Firefox, for example, followed by History to view the recently visited web pages.

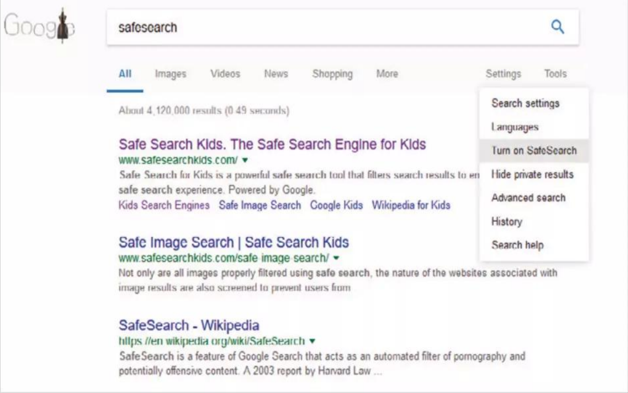


Name	Tags	Location
Google		https://www.google.co.uk/
Utp Cable Connection Laptop Stock Pho...		https://www.shutterstock.com/image-photo/...
Unplug Ethernet Stock Images, Royalty-...		https://www.shutterstock.com/search?search...
Father Using Computer Son Family Back...		https://www.shutterstock.com/image-photo/...
Living Room Computer Stock Images, R...		https://www.shutterstock.com/search?search...
Isp Internet Service Provider White Text ...		https://www.shutterstock.com/image-vector...
Isp Stock Images, Royalty-Free Images ...		https://www.shutterstock.com/search?search...
isp - Google Search		https://www.google.co.uk/search?q=rules&s...
isps - Google Search		https://www.google.co.uk/search?q=rules&s...
Stamp Word Dos Donts Grunge Style Sto...		https://www.shutterstock.com/image-vector...
Dos Donts Stock Photo 570990148 - Shut...		https://www.shutterstock.com/image-photo/...
do and don'ts - Google Search		https://www.google.co.uk/search?q=rules&s...
do's and don ts png - Google Search		https://www.google.co.uk/search?safe=off&...
do's and don ts png · Google Search		https://www.google.co.uk/search?safe=off&...
Google Search		https://www.google.co.uk/search?tbs=sbi:A...
do and don'ts - Google Search		https://www.google.co.uk/search?q=rules&s...
Dos And Don&#39;ts Stock Images, Roy...		https://www.shutterstock.com/search?search...

Name: Today

PARENTAL FILTERS

Make sure that any search engines used, such as Google, have the parental filters set to the maximum or strict levels. In Google, enter something in the search box, then click the Settings link and turn on SafeSearch. Other search engines may differ in appearance but they all have some form of customisable filter rule.



About 4,120,000 results (0.49 seconds)

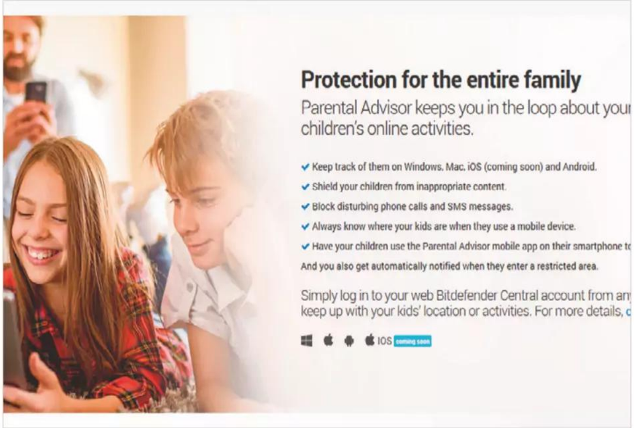
Safe Search Kids. The Safe Search Engine for Kids
www.safesearchkids.com/
Safe Search for Kids is a powerful safe search tool that filters search results to en
safe search experience. Powered by Google.
Kids Search Engines   Safe Image Search   Google Kids   Wikipedia for Kids

Safe Image Search | Safe Search Kids
www.safesearchkids.com/safe image search/
Not only are all images properly filtered using safe search, the nature of the websites associated with image results are also screened to prevent users from

SafeSearch - Wikipedia
https //en wikipedia org/wiki/SafeSearch
SafeSearch is a feature of Google Search that acts as an automated filter of pornography and potentially offensive content. A 2003 report by Harvard Law ...

3RD PARTY SECURITY

It's worth investing in a third-party anti-malware security suite, such as Bitdefender. With Bitdefender, and other security suites, you get some form of family protection allowing you to keep track of Internet use, block unknown communications and even extend the protection to mobile devices.



Protection for the entire family

Parental Advisor keeps you in the loop about your children's online activities.

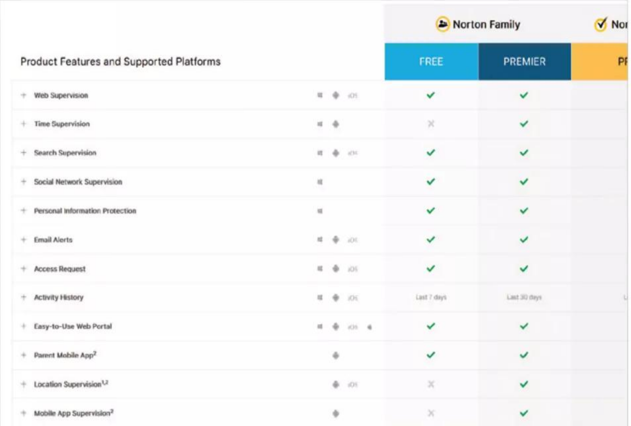
- ✓ Keep track of them on Windows, Mac, iOS (coming soon) and Android.
- ✓ Shield your children from inappropriate content.
- ✓ Block disturbing phone calls and SMS messages.
- ✓ Always know where your kids are when they use a mobile device.
- ✓ Have your children use the Parental Advisor mobile app on their smartphone t

And you also get automatically notified when they enter a restricted area.

Simply log in to your web Bitdefender Central account from an keep up with your kids' location or activities. For more details, c

FREE MONITORING

If you don't want to pay for a full suite, consider using a free monitoring and protection tool such as Norton Family Free Edition. With it you can supervise web access, protect personal information and set up social network supervision.



	Norton Family	
Product Features and Supported Platforms	FREE	PREMIER
Web Supervision	✓	✓
Time Supervision	✗	✓
Search Supervision	✓	✓
Social Network Supervision	✓	✓
Personal Information Protection	✓	✓
Email Alerts	✓	✓
Access Request	✓	✓
Activity History	Last 7 days	Last 30 days
Easy-to-Use Web Portal	✓	✓
Parent Mobile App[2]	✓	✓
Location Supervision[1,2]	✗	✓
Mobile App Supervision[2]	✗	✓

BECOME FRIENDS

If your child has any social media accounts, make sure to become friends or connected to them. This way you can see what they post, what they like and be ready to help them should something ever get out of hand.

Tips for Technical Guardians to Monitor a Child's Online Activity

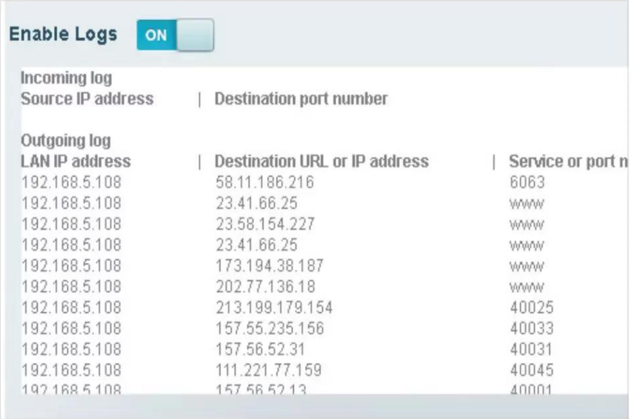
For those parents and guardians who are more technically minded, there's a wealth of software and features available that enable you to monitor your child's Internet activities. Some are simple solutions, others require a little more work, it depends what you're looking for.

Ten Steps for Tech Minded Guardians

As a technically minded parent or guardian, you can monitor traffic, set up batch files to send daily connection reports and fiddle with the inner workings of your router. Here are ten tips to help you out.

ROUTER LOGS

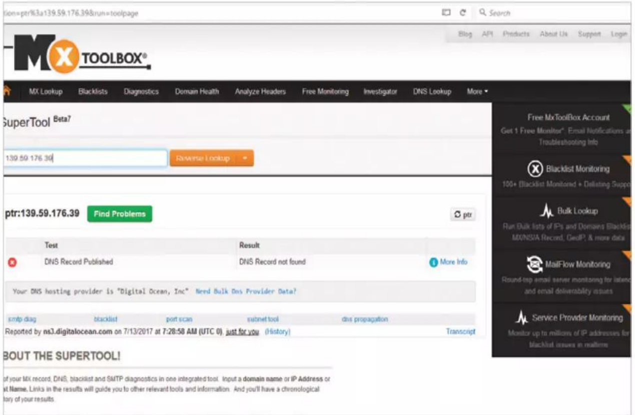
Depending on the router you own, either one you've bought or the ISP-provided one, there's often a way to log web traffic. The logging can sometimes be a single entry detailing the entire house's activity or you can specify individual devices connected to the router. You need to consult your router guide for more information, or contact your ISP.


Enable Logs
ON

```
Incoming log
Source IP address      | Destination port number

Outgoing log
LAN IP address         | Destination URL or IP address    | Service or port n
192.168.5.108            58.11.186.216                      6063
192.168.5.108            23.41.66.25                        www
192.168.5.108            23.58.154.227                      www
192.168.5.108            23.41.66.25                        www
192.168.5.108            173.194.38.187                     www
192.168.5.108            202.77.136.18                      www
192.168.5.108            213.199.179.154                    40025
192.168.5.108            157.55.235.156                     40033
192.168.5.108            157.56.52.31                       40031
192.168.5.108            111.221.77.159                     40045
192.168.5.108            157.56.52.13                       40001
```

RESOLVE ADDRESSES

If when consulting router logs you have countless IP addresses instead of domain names, you can run the addresses through a reverse IP lookup site. There are dozens available, but MX Toolbox is a good place to start. Enter the IP address and you can see who the hosting company is, and from there ascertain what's being viewed.


MX TOOLBOX
Blog
API
Products
About Us
Support
Login
MX Lookup
Blacklists
Diagnostics
Domain Health
Analyze Headers
Free Monitoring
Investigator
DNS Lookup
More
SuperTool Beta7
Reverse Lookup
Find Problems
ptr
More Info
smtp diag
blacklist
port scan
subnet tool
dns propagation
Transcript
Free MxToolBox Account
Blacklist Monitoring
Bulk Lookup
MailFlow Monitoring
Service Provider Monitoring

139.59.176.39

ptr:139.59.176.39

Test	Result
DNS Record Published	DNS Record not found

Your DNS hosting provider is "Digital Ocean, Inc" Need Bulk Dns Provider Data?

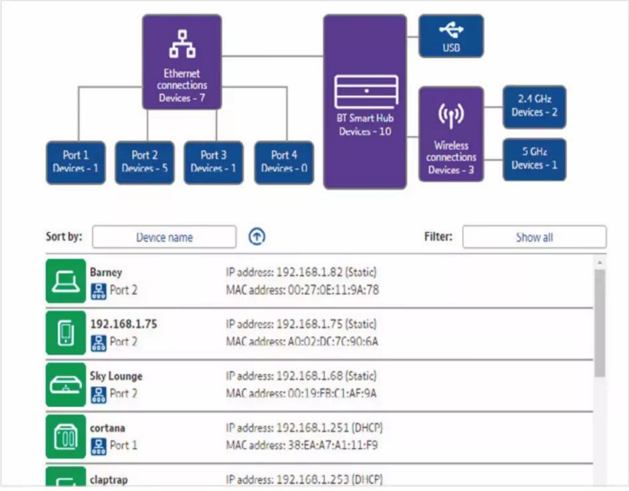
Reported by ns3.digitalocean.com on 7/13/2017 at 7:28:58 AM (UTC 0). just for you (History)

BOUT THE SUPERTOOL!

of your MX record, DNS, blacklist and SMTP diagnostics in one integrated tool. Input a domain name or IP Address or t Name. Links in the results will guide you to other relevant tools and information. And you'll have a chronological tory of your results.

FRIENDLY NAMING

This may seem an obvious step but it's one that often overlooked. If you're going to monitor online activity, you need to make sure that the child's devices are correctly labelled in the router setup. Instead of them being just a string of numbers, take the time to ensure they're labelled as 'Bobby's iPad' and so on.

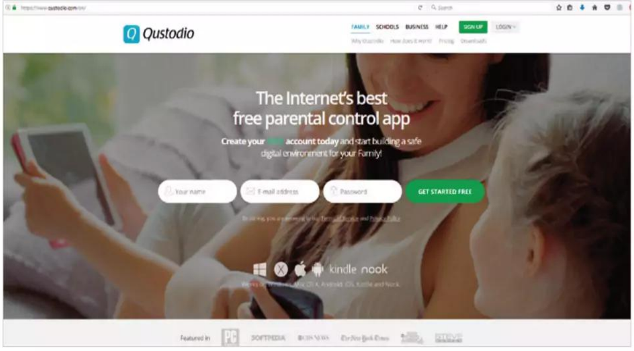

Ethernet connections Devices - 7
BT Smart Hub Devices - 10
USB
Wireless connections Devices - 3
2.4 GHz Devices - 2
5 GHz Devices - 1
Port 1 Devices - 1
Port 2 Devices - 5
Port 3 Devices - 1
Port 4 Devices - 0

Sort by: Device name
Filter: Show all

Barney Port 2	IP address: 192.168.1.82 (Static) MAC address: 00:27:0E:11:9A:78
192.168.1.75 Port 2	IP address: 192.168.1.75 (Static) MAC address: A0:02:DC:7C:90:6A
Sky Lounge Port 2	IP address: 192.168.1.68 (Static) MAC address: 00:19:FB:C1:AF:9A
cortana Port 1	IP address: 192.168.1.251 (DHCP) MAC address: 38:EA:A7:A1:11:F9
claptrap	IP address: 192.168.1.253 (DHCP)

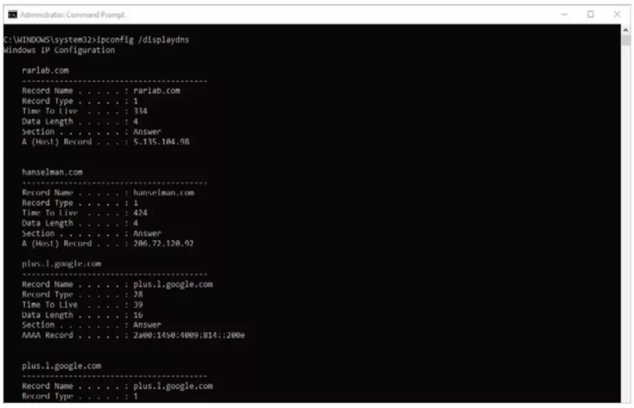
PARENTAL MONITORING

Monitoring software is a must have for parents or guardians who want to limit and control what their children do online. We'll look at some examples over the page but to begin with take a look at Qustodio Parental Control: **https://. qustodio.com/en/**. It's a cross-platform tool for better monitoring of online activity, and it's reasonably well priced.


Qustodio
FAMILY
SCHOOLS
BUSINESS
HELP
SIGN UP
LOGIN
The Internet's best free parental control app
Create your account today and start building a safe digital environment for your Family!
Your name
E-mail address
Password
GET STARTED FREE
kindle nook
Featured in

DISPLAY DNS

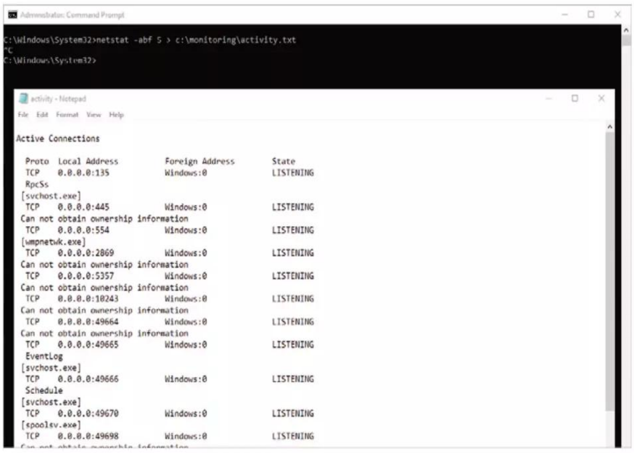
For those who like to get their hands dirty in the command line, open up CMD from the Windows Start button and enter the command: **ipconfig /displaydns**. This will list the sites visited by the user during their session. If you want, record the sites to a text file for viewing later with, for example: **ipconfig /displaydns > c:\monitoring\sites.txt**.


Administrator: Command Prompt

```
C:\WINDOWS\system32>ipconfig /displaydns
Windows IP Configuration

    rarlab.com
    ----------------------------------------
    Record Name . . . . . : rarlab.com
    Record Type . . . . . : 1
    Time To Live  . . . . : 334
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 5.135.104.98


    hanselman.com
    ----------------------------------------
    Record Name . . . . . : hanselman.com
    Record Type . . . . . : 1
    Time To Live  . . . . : 424
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 206.72.120.92

    plus.l.google.com
    ----------------------------------------
    Record Name . . . . . : plus.l.google.com
    Record Type . . . . . : 28
    Time To Live  . . . . : 39
    Data Length . . . . . : 16
    Section . . . . . . . : Answer
    AAAA Record . . . . . : 2a00:1450:4009:814::200e


    plus.l.google.com
    ----------------------------------------
    Record Name . . . . . : plus.l.google.com
    Record Type . . . . . : 1
```

NETSTAT COMMAND

Using the Netstat command that we looked at on page 98, you can enter into a command prompt: **netstat -abf 5 > c:\monitoring\activity.txt**. This will record the entire activity of a session to a file, which you can then browse. The recording will stop once the child has logged out of their Windows account.

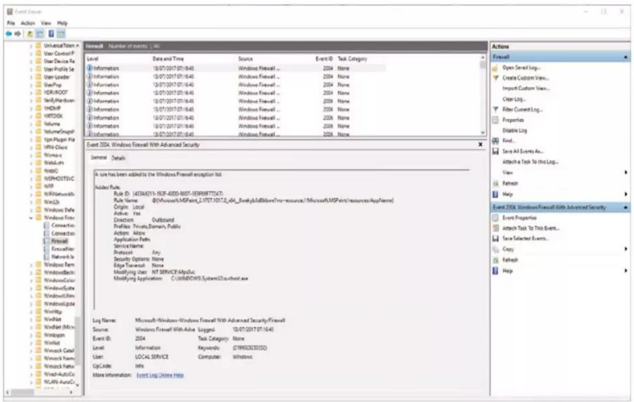

Administrator: Command Prompt
activity - Notepad
File
Edit
Format
View
Help

```
C:\Windows\System32>netstat -abf 5 > c:\monitoring\activity.txt
^C
C:\Windows\System32>
```

```
Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            Windows:0              LISTENING
  RpcSs
 [svchost.exe]
  TCP    0.0.0.0:445            Windows:0              LISTENING
 Can not obtain ownership information
  TCP    0.0.0.0:554            Windows:0              LISTENING
 [wmpnetwk.exe]
  TCP    0.0.0.0:2869           Windows:0              LISTENING
 Can not obtain ownership information
  TCP    0.0.0.0:5357           Windows:0              LISTENING
 Can not obtain ownership information
  TCP    0.0.0.0:10243          Windows:0              LISTENING
 Can not obtain ownership information
  TCP    0.0.0.0:49664          Windows:0              LISTENING
 Can not obtain ownership information
  TCP    0.0.0.0:49665          Windows:0              LISTENING
  EventLog
 [svchost.exe]
  TCP    0.0.0.0:49666          Windows:0              LISTENING
  Schedule
 [svchost.exe]
  TCP    0.0.0.0:49670          Windows:0              LISTENING
 [spoolsv.exe]
  TCP    0.0.0.0:49698          Windows:0              LISTENING
```

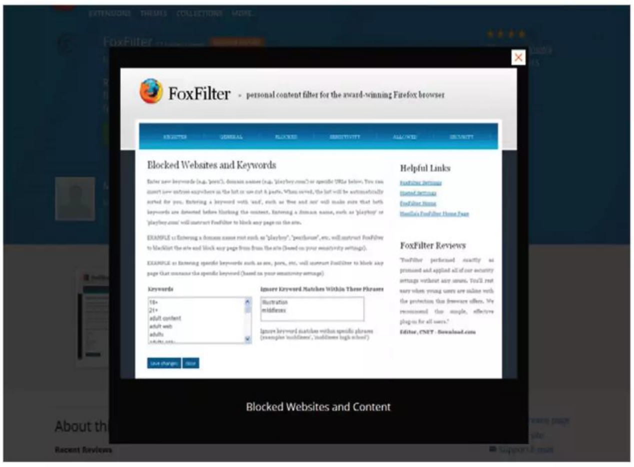
WINDOWS LOGS

Don't forget to check your Windows Event Logs, especially the Windows Firewall Event Log for any activity that may have triggered the Firewall. You can then build up a picture of where the child is visiting that's causing the Firewall to react and educate them in the dangers of malware and such.



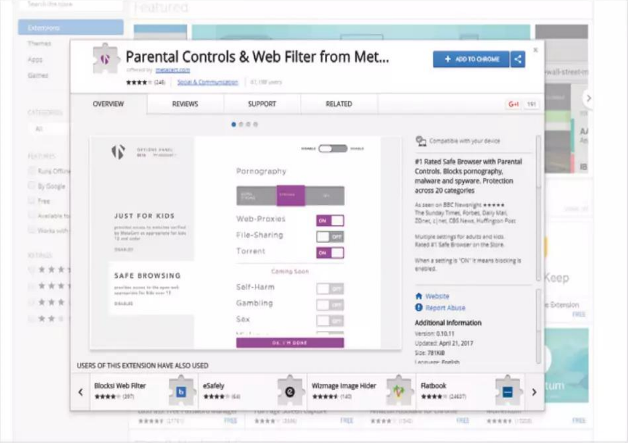
BROWSER CONTROL

If you need a specific monitoring and parental control tool, then consider using FoxFilter for Firefox. This is an add-on that can block customised websites, such as anything containing inappropriate content and report its use in a handy web interface.


FoxFilter
Blocked Websites and Keywords
Helpful Links
FoxFilter Reviews
Blocked Websites and Content

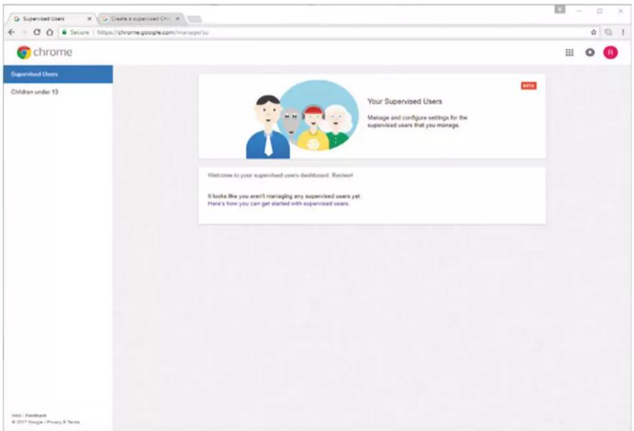
CHROME CONTROL

Users of Chrome can try MetaCert's Parental Controls & Web Filtering add-on. With it you can block certain sites, set profiles and monitor the web activity of your child as they use the browser. There are plenty of features, so it's worth looking over if you regularly use Chrome.


Parental Controls & Web Filter from Met...
+ ADD TO CHROME
OVERVIEW
REVIEWS
SUPPORT
RELATED
JUST FOR KIDS
SAFE BROWSING
Pornography
Web-Proxies
File-Sharing
Torrent
Self-Harm
Gambling
Sex
USERS OF THIS EXTENSION HAVE ALSO USED

SUPERVISED USER

While still on Chrome users, if you visit **http://chrome.com/manage**, you're able to set up a supervised user for the other Chrome accounts. This way you can set restrictions and monitor the sites that a user has visited during their Chrome use.


chrome
Your Supervised Users

Ten Monitoring Tools to Install and Use

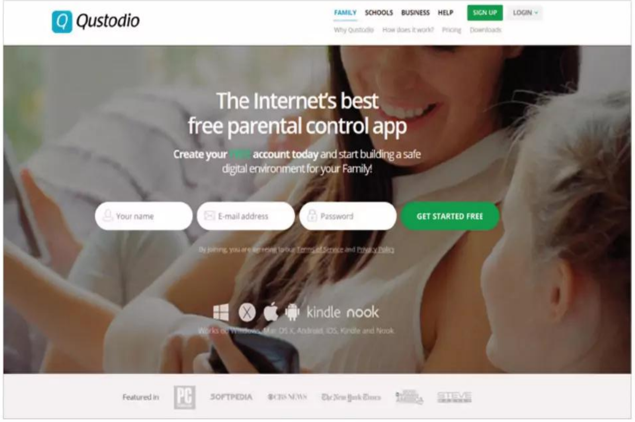
Monitoring tools usually come within a complete Parental Control package. These tools can be dedicated programs, or come as a part of a security suite. Either way, they're excellent ways to help keep children and young people safe on the Internet.

Parental Controls

We've collated ten of the better parental control and monitoring tools and software, in no particular order. Some offer their software for free, others you need to pay for.

QUSTODIO

We've mentioned Qustodio in the previous page, so it's a good example to kick of this top ten tools section with. Qustodio is a complete package that monitors, blocks, filters and controls times, games and apps across many different platforms. Pricing for up to five devices starts at £32.95 per year.

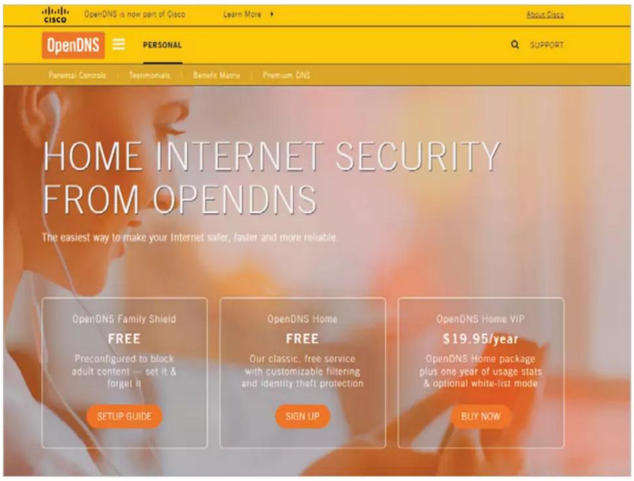

Qustodio
FAMILY
SCHOOLS
BUSINESS
HELP
SIGN UP
LOGIN
Your name
E-mail address
Password
GET STARTED FREE
kindle
nook
Featured in

The Internet's best free parental control app

Create your [illegible] account today and start building a safe digital environment for your Family!

OPENDNS

OpenDNS from Cisco offers both free and paid-for services to help block inappropriate content across virtually any Internet connected device. You need to set up DNS entries in your router to take advantage of it but full instructions are given via a helpful setup guide.


CISCO
OpenDNS is now part of Cisco
Learn More
About Cisco
OpenDNS
PERSONAL
SUPPORT
Parental Controls
Testimonials
Benefit Matrix
Premium DNS
SETUP GUIDE
SIGN UP
BUY NOW

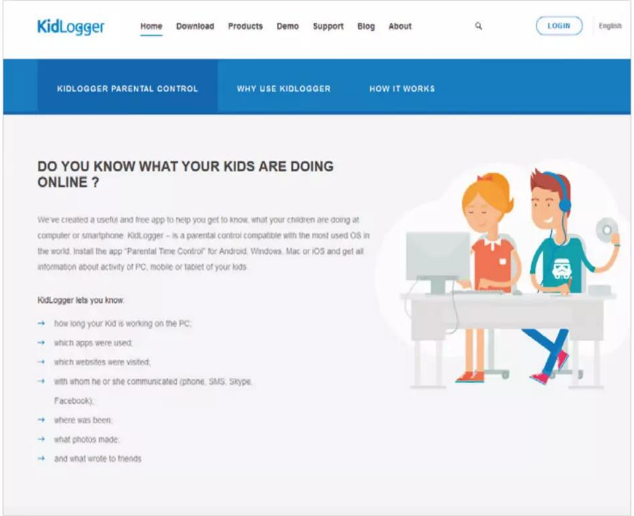
HOME INTERNET SECURITY FROM OPENDNS

The easiest way to make your Internet safer, faster and more reliable.

OpenDNS Family Shield	OpenDNS Home	OpenDNS Home VIP
FREE	FREE	$19.95/year
Preconfigured to block adult content — set it & forget it	Our classic, free service with customizable filtering and identity theft protection	OpenDNS Home package plus one year of usage stats & optional white-list mode

KIDLOGGER

KidLogger is an interesting product that offers a basic, single device with nine days of history for free, moving up to five devices, then ten devices for increasing costs. You can monitor browser activities across Windows, Mac and Android; block apps, take screenshots and limit time, amongst other features.


KidLogger
Home
Download
Products
Demo
Support
Blog
About
LOGIN
English
KIDLOGGER PARENTAL CONTROL
WHY USE KIDLOGGER
HOW IT WORKS

DO YOU KNOW WHAT YOUR KIDS ARE DOING ONLINE ?

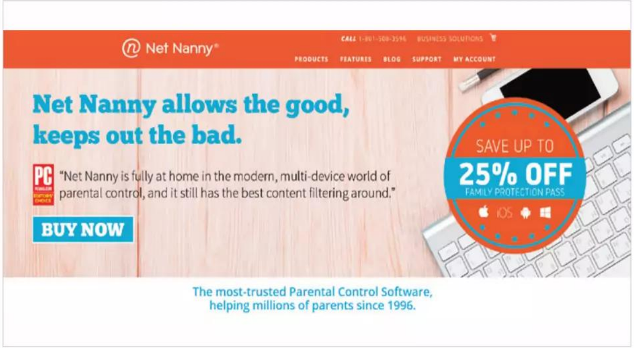
We've created a useful and free app to help you get to know, what your children are doing at computer or smartphone. KidLogger – is a parental control compatible with the most used OS in the world. Install the app "Parental Time Control" for Android, Windows, Mac or iOS and get all information about activity of PC, mobile or tablet of your kids.

KidLogger lets you know:

- how long your Kid is working on the PC;
- which apps were used;
- which websites were visited;
- with whom he or she communicated (phone, SMS, Skype, Facebook);
- where was been;
- what photos made;
- and what wrote to friends

NET NANNY

Without a doubt, one of the most respected parental control solutions available is Net Nanny. It's been around since 1996 and offers unparalleled levels of filtering, protection, monitoring and parental controls. It's cross-platform and prices vary depending on what you want, so it's best to check out the latest offers available.


Net Nanny®
BUSINESS SOLUTIONS
PRODUCTS
FEATURES
BLOG
SUPPORT
MY ACCOUNT
PC
BUY NOW
SAVE UP TO
25% OFF
FAMILY PROTECTION PASS
iOS

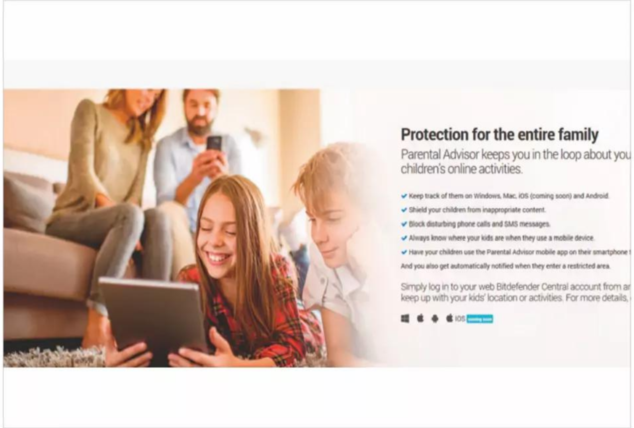
Net Nanny allows the good, keeps out the bad.

"Net Nanny is fully at home in the modern, multi-device world of parental control, and it still has the best content filtering around."

The most-trusted Parental Control Software, helping millions of parents since 1996.

BITDEFENDER

Bitdefender's Total Security suite offers an excellent parental control and monitoring tool within it's already impressive list of features. It's cross-platform, can shield children and young people from inappropriate content and extends its use to mobile devices too. Pricing starts at just £34.99.



Protection for the entire family

Parental Advisor keeps you in the loop about you children's online activities.

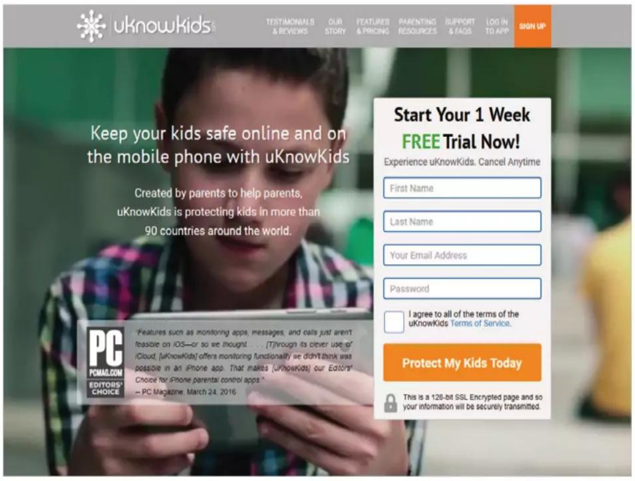
- ✓ Keep track of them on Windows, Mac, iOS (coming soon) and Android.
- ✓ Shield your children from inappropriate content.
- ✓ Block disturbing phone calls and SMS messages.
- ✓ Always know where your kids are when they use a mobile device.
- ✓ Have your children use the Parental Advisor mobile app on their smartphone

And you also get automatically notified when they enter a restricted area.

Simply log in to your web Bitdefender Central account from ar keep up with your kids' location or activities. For more details,

UKNOWKIDS

uKnowKids provides a wealth of features for parents, including call logging on devices (with Facetime call logs), image reviews that children post, social media monitoring and web browsing history access and controls to block inappropriate content. Pricing varies, so it's best to visit the uKnowKids site to see the latest offers available.



uknowkids
TESTIMONIALS & REVIEWS
OUR STORY
FEATURES & PRICING
PARENTING RESOURCES
SUPPORT & FAQS
LOG IN TO APP
SIGN UP

Keep your kids safe online and on the mobile phone with uKnowKids

Created by parents to help parents, uKnowKids is protecting kids in more than 90 countries around the world.

"Features such as monitoring apps, messages, and calls just aren't feasible on iOS—or so we thought. . . . [T]hrough its clever use of iCloud, [uKnowKids] offers monitoring functionality we didn't think was possible in an iPhone app. That makes [uKnowKids] our Editors' Choice for iPhone parental control apps."
– PC Magazine, March 24, 2016

PC
PCMAG.COM
EDITORS' CHOICE

Start Your 1 Week FREE Trial Now!

Experience uKnowKids. Cancel Anytime

First Name

Last Name

Your Email Address

Password

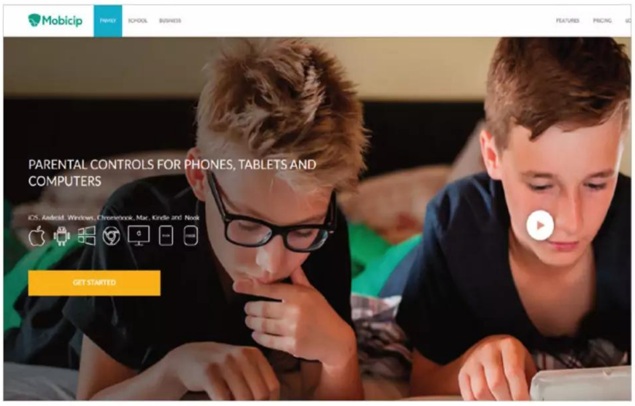
☐ I agree to all of the terms of the uKnowKids Terms of Service.

Protect My Kids Today

This is a 128-bit SSL Encrypted page and so your information will be securely transmitted.

MOBICIP

Mobicip is a cross-platform tool that offers app monitoring, web browsing monitoring, time limits and custom filters. The basic package is free but has some good features on offer, whilst the premium package costs $39.99 per year.



Mobicip
FEATURES
PRICING

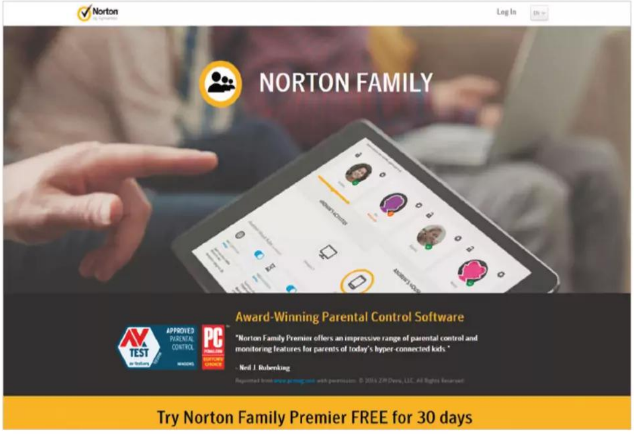
PARENTAL CONTROLS FOR PHONES, TABLETS AND COMPUTERS

iOS, Android, Windows, Chromebook, Mac, Kindle and Nook

GET STARTED

NORTON FAMILY

Norton Family is a previously mentioned tool that offers both free and paid for services to help protect children and young people online. It's cross-platform, provides protection for social media accounts, time supervision, activity monitoring and much more. Check the site for the latest features and pricing.



Norton
Log In
NORTON FAMILY
AV TEST
APPROVED PARENTAL CONTROL
PC
EDITORS' CHOICE

Award-Winning Parental Control Software

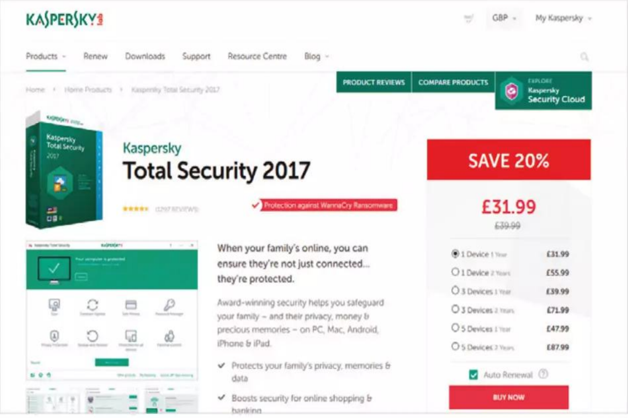
"Norton Family Premier offers an impressive range of parental control and monitoring features for parents of today's hyper-connected kids."

- Neil J. Rubenking

Try Norton Family Premier FREE for 30 days

KASPERSKY

Kaspersky Total Security 2017/8, very much like Bitdefender, offers a parental control feature within its security suite. With it the parent or guardian can set time restrictions, block access to inappropriate content, monitor Internet activities and monitor communications on mobile devices. Prices start at just £31.99 per year for a single device.



KASPERSKY
GBP
My Kaspersky
Products
Renew
Downloads
Support
Resource Centre
Blog
PRODUCT REVIEWS
COMPARE PRODUCTS
EXPLORE Kaspersky Security Cloud

Kaspersky
Total Security 2017

Protection against WannaCry Ransomware

When your family's online, you can ensure they're not just connected... they're protected.

Award-winning security helps you safeguard your family – and their privacy, money & precious memories – on PC, Mac, Android, iPhone & iPad.

- ✓ Protects your family's privacy, memories & data
- ✓ Boosts security for online shopping & banking

SAVE 20%

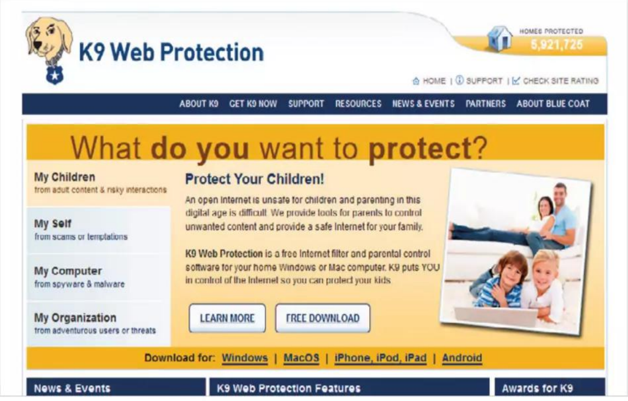
£31.99
~~£39.99~~

● 1 Device £31.99
○ 1 Device £55.99
○ 3 Devices £39.99
○ 3 Devices £71.99
○ 5 Devices £47.99
○ 5 Devices £87.99

☑ Auto Renewal

K9 WEB PROTECTION

K9 Web Protection (nothing to do with protecting dogs from accessing the Internet) is a free, cloud-based Internet filter that blocks inappropriate content, sets time restrictions, forces safe search on all search engines and works on both Windows and Mac computers.



K9 Web Protection
HOMES PROTECTED
5,921,725
HOME | SUPPORT | CHECK SITE RATING
ABOUT K9
GET K9 NOW
SUPPORT
RESOURCES
NEWS & EVENTS
PARTNERS
ABOUT BLUE COAT

What do you want to protect?

My Children
from adult content & risky interactions

My Self
from scams or temptations

My Computer
from spyware & malware

My Organization
from adventurous users or threats

Protect Your Children!

An open Internet is unsafe for children and parenting in this digital age is difficult. We provide tools for parents to control unwanted content and provide a safe Internet for your family.

K9 Web Protection is a free Internet filter and parental control software for your home Windows or Mac computer. K9 puts YOU in control of the Internet so you can protect your kids.

LEARN MORE
FREE DOWNLOAD

Download for: Windows | MacOS | iPhone, iPod, iPad | Android

News & Events
K9 Web Protection Features
Awards for K9

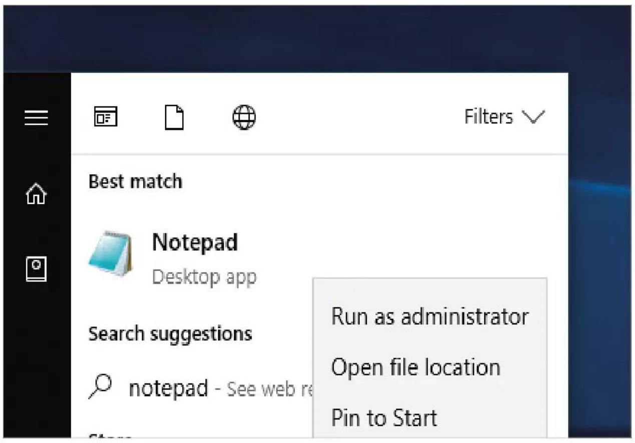
Using the Windows Hosts File to Block Sites

The Hosts file is used by the operating system to map hostnames to IP addresses. It's a historical file that's used by Windows to signpost internal and external websites, and other such networking services. You can use it to your advantage though.

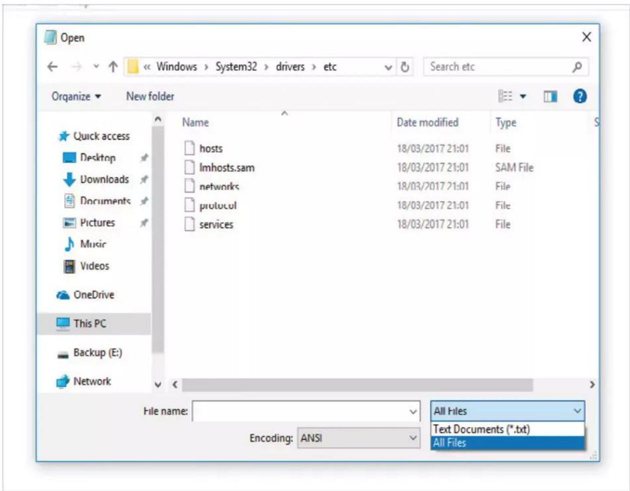
The Perfect Host

The Hosts file is simply a plain text file for mapping network locations and is checked by Windows to see if there's an entry whenever the user requests access to a website or network resource. Here's how to block websites using it.

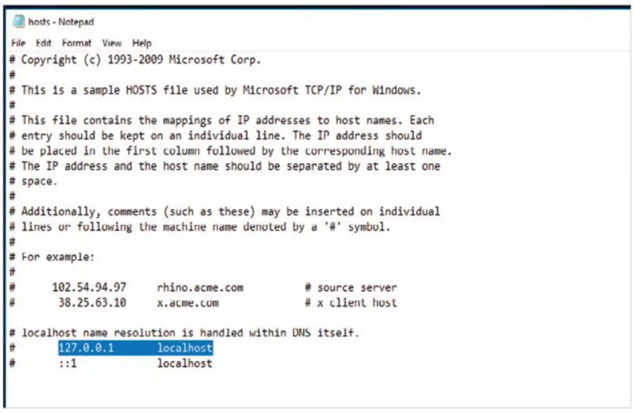
STEP 1 First you need to open the Hosts file with administrative access. To do this, click on the Windows Start button and type notepad. When Notepad appears in the search list, right-click it and choose Run as Administrator from the menu and click Yes for the UAC message authentication.


Filters
Best match
Notepad
Desktop app
Search suggestions
notepad - See web re
Run as administrator
Open file location
Pin to Start

STEP 2 Within Notepad click File > Open and navigate to c:\Windows\System32\drivers\etc. Click the drop-down menu saying Text Documents and change it to All Files. This will list the files within the etc folder. Click on the Hosts file, then click the Open button.

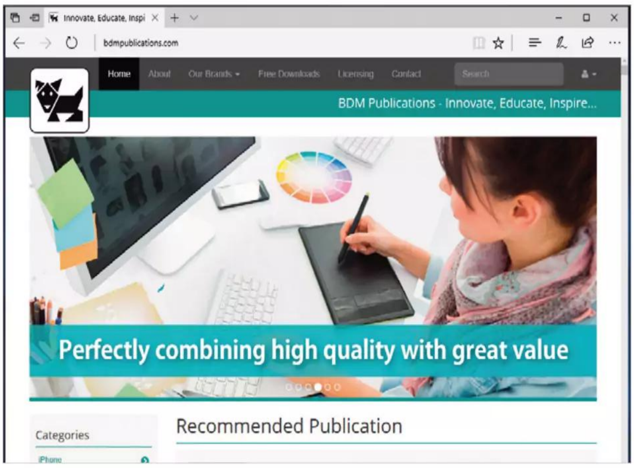

Open
« Windows › System32 › drivers › etc
Search etc
Organize
New folder
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
Backup (E:)
Network
Name
Date modified
Type
hosts
18/03/2017 21:01
File
lmhosts.sam
18/03/2017 21:01
SAM File
networks
18/03/2017 21:01
File
protocol
18/03/2017 21:01
File
services
18/03/2017 21:01
File
File name:
Encoding: ANSI
All Files
Text Documents (*.txt)
All Files

STEP 3 You can see that the Hosts file is a historic text file dating back from the early days of networking and communications. The localhost entry at the bottom of the file, 127.0.0.1 is your computer. This is the important entry, as we're going to fool the networking services into believing that a website is stored locally.

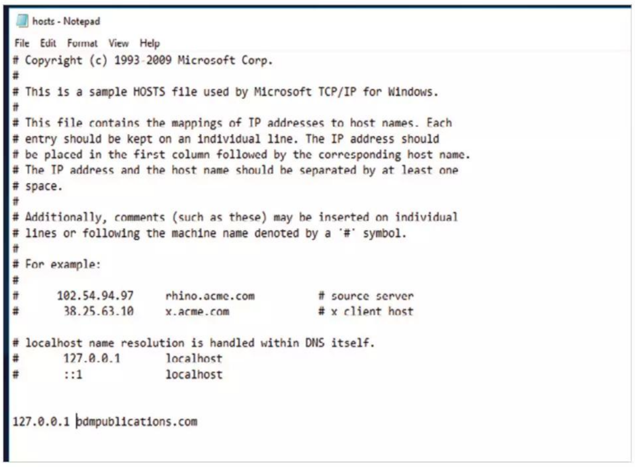

hosts - Notepad
File Edit Format View Help

```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost
```

STEP 4 It's this fooling Windows that makes this such an effective solution to blocking sites, as you're not fiddling with your router or other networking devices. Let's say, for example, you want to block BDM Publications. Open a browser and go to the BDM Publications website, **https://bdmpublications.com**.

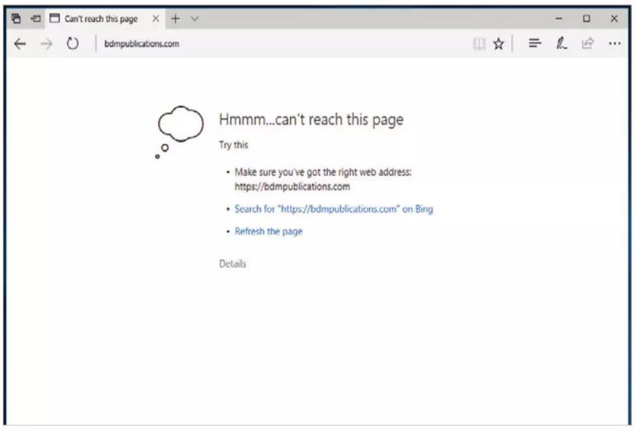

Innovate, Educate, Inspi
bdmpublications.com
Home
About
Our Brands
Free Downloads
Licensing
Contact
Search
BDM Publications - Innovate, Educate, Inspire...
Perfectly combining high quality with great value
Categories
Recommended Publication

STEP 5 Either close or minimise the browser window and get back to the Hosts file in Notepad. Press Enter a couple of times to start a new line under the last hash and type in: **127.0.0.1 bdmpublications.com**. Don't add the HTTPS or the www part, just as it appears in the address bar.


hosts - Notepad
File Edit Format View Help

```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost


127.0.0.1 bdmpublications.com
```

STEP 6 In Notepad, click File > Save, to obviously save the newly edited Hosts file. Now get back to your browser and either refresh the page or close and reload the browser. When back up, in the address bar enter the site: **https://bdmpublications.com**. You can now see that the page won't load.


Can't reach this page
bdmpublications.com

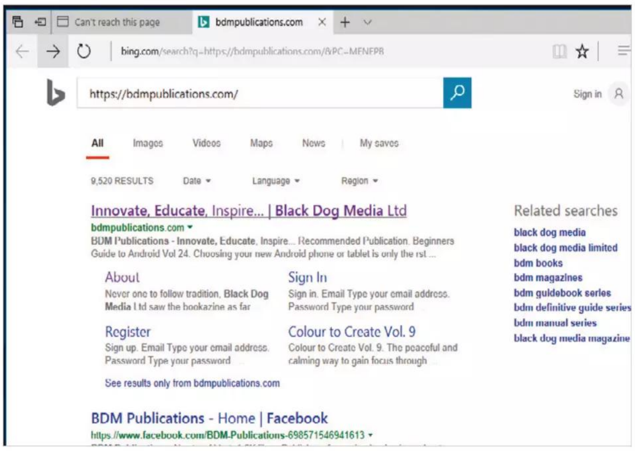
Hmmm...can't reach this page

Try this

- Make sure you've got the right web address: https://bdmpublications.com
- Search for "https://bdmpublications.com" on Bing
- Refresh the page

Details

STEP 7 You can try searching for it via Google or Bing but it still won't load as you've successfully blocked access to the website's hostname from the Hosts file. You can also see that any sub-domains after the main bdmpublications.com address are also blocked, which is certainly handy for some sites.


Can't reach this page
bdmpublications.com
bing.com/search?q=https://bdmpublications.com/&PC=MFNFPB
https://bdmpublications.com/
Sign in
All
Images
Videos
Maps
News
My saves
9,520 RESULTS
Date
Language
Region

Innovate, Educate, Inspire... | Black Dog Media Ltd
bdmpublications.com
BDM Publications - Innovate, Educate, Inspire... Recommended Publication. Beginners Guide to Android Vol 24. Choosing your new Android phone or tablet is only the rst ...

About
Never one to follow tradition, Black Dog Media Ltd saw the bookazine as far

Sign In
Sign in. Email Type your email address. Password Type your password

Register
Sign up. Email Type your email address. Password Type your password

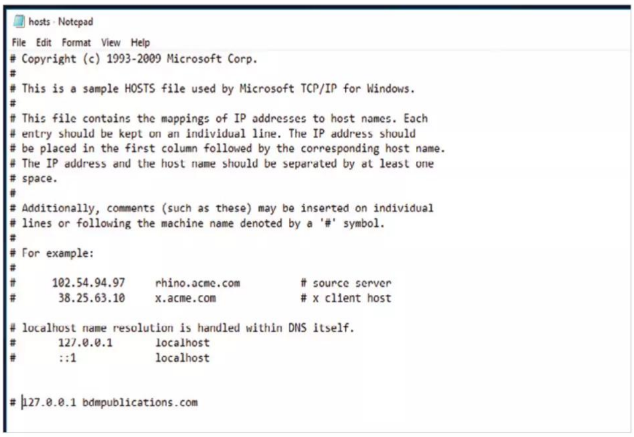
Colour to Create Vol. 9
Colour to Create Vol. 9. The peaceful and calming way to gain focus through

See results only from bdmpublications.com

BDM Publications - Home | Facebook
https://www.facebook.com/BDM-Publications-698571546941613

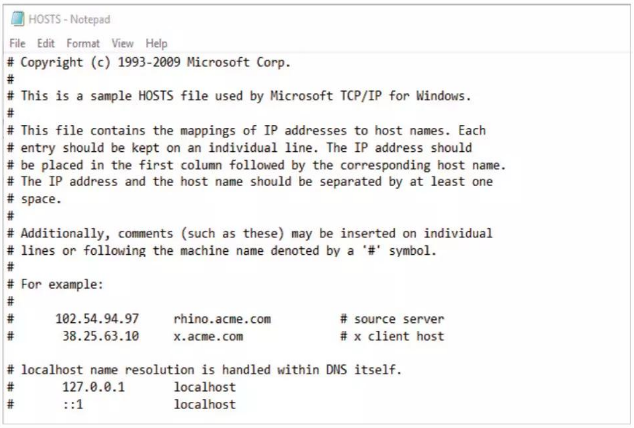
Related searches
black dog media
black dog media limited
bdm books
bdm magazines
bdm guidebook series
bdm definitive guide series
bdm manual series
black dog media magazine

STEP 8 What we've done here is fool Windows' networking services into thinking that the website bdmpublications.com, is being hosted on the computer itself and not out there on the Internet. If we wanted to remove the block, we can simply delete the line or put a hash at the start of the line and save the file.


hosts - Notepad
File Edit Format View Help

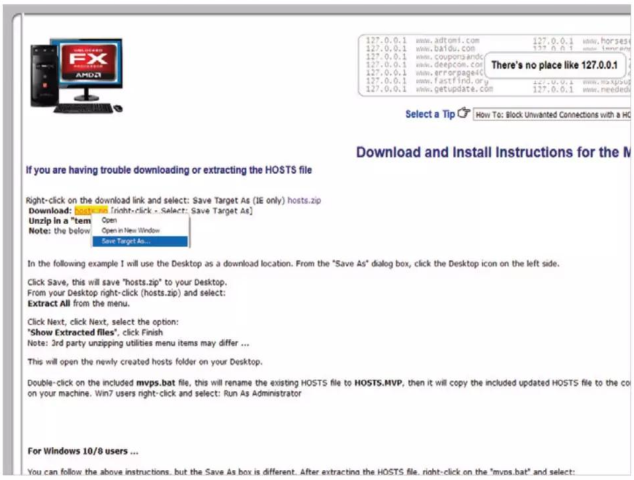
```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost


# 127.0.0.1 bdmpublications.com
```

STEP 9 Over time you can add more sites to the Hosts file list, pointing each one back to the 127.0.0.1 address of the local computer to block it from ever being reached; even if you use a different browser or other Internet accessible program.


HOSTS - Notepad
File Edit Format View Help

```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost
```

STEP 10 If you want a complete list that's already been created, then WinHelp2002 provides a downloadable compressed Hosts file that you can replace your own with. You can find it at **http://winhelp2002.mvps.org/hosts2.htm**; just read the instructions to replace the new Hosts file.


FX
AMD
127.0.0.1 www.adtomi.com
127.0.0.1 www.baidu.com
127.0.0.1 www.couponsandc
127.0.0.1 www.deepcom.com
127.0.0.1 www.errorpage4
127.0.0.1 www.fastfind.org
127.0.0.1 www.getupdate.com
127.0.0.1 www.horses
127.0.0.1 www.needed
There's no place like 127.0.0.1
Select a Tip
How To: Block Unwanted Connections with a HO
Open
Open in New Window
Save Target As...

Download and Install Instructions for the M

If you are having trouble downloading or extracting the HOSTS file

Right-click on the download link and select: Save Target As (IE only) hosts.zip
Download: hosts.zip [right-click - Select: Save Target As]
Unzip in a "tem
Note: the below

In the following example I will use the Desktop as a download location. From the "Save As" dialog box, click the Desktop icon on the left side.

Click Save, this will save "hosts.zip" to your Desktop.
From your Desktop right-click (hosts.zip) and select:
Extract All from the menu.

Click Next, click Next, select the option:
"**Show Extracted files**", click Finish
Note: 3rd party unzipping utilities menu items may differ ...

This will open the newly created hosts folder on your Desktop.

Double-click on the included **mvps.bat** file, this will rename the existing HOSTS file to **HOSTS.MVP**, then it will copy the included updated HOSTS file to the co
on your machine. Win7 users right-click and select: Run As Administrator

For Windows 10/8 users ...

You can follow the above instructions, but the Save As box is different. After extracting the HOSTS file, right-click on the "mvps.bat" and select:

Further Protection for Young Adults

Younger children are certainly vulnerable when on the Internet but from 13-years a teenager is allowed to have a Facebook, Twitter and other social media accounts. This opens up a whole new level of online protection issues and significant dangers within.

We look at how you can help protect their social media status and how to create their own Windows accounts.

168 Staying Safe with Facebook for Teens
170 Staying Safe with Twitter for Teens
172 Staying Safe with Instagram for Teens
174 Staying Safe with WhatsApp for Teens
176 Staying Safe with Snapchat for Teens
178 Creating a Child Account in Windows 10
180 Windows 10 Family Features
182 Problems with In-app Spending
184 Tips on How to Stop In-app Overspending
186 Online Child Safety at School
188 Where to Find Help with Online Child Safety
190 What the Experts Say
192 Glossary of Terms

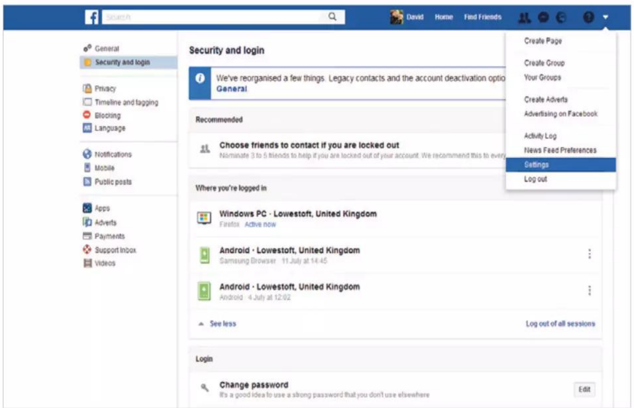
Staying Safe with Facebook for Teens

If your child is thirteen they're now, according to the rules of the company, allowed to have a Facebook account. Facebook's popularity has waned in recent years with teens but it's still heavily used. Therefore, we need to make sure that our teens are safe when on it.

Smells Like Teen Facebook

Providing you adhere to the recommended security settings for Facebook, and don't add just anyone who sends you a friend request, you should be relatively safe. However, these ten tips will help.

Get to the Facebook security settings by clicking on the Down Arrow next to the question mark in the top right of the Facebook interface. From there click the Settings option on the menu and then Security and login on the left-hand panel. If you haven't already, make sure you're using a strong password, as suggested earlier in this book.


Search
David
Home
Find Friends
General
Security and login
Privacy
Timeline and tagging
Blocking
Language
Notifications
Mobile
Public posts
Apps
Adverts
Payments
Support Inbox
Videos
Create Page
Create Group
Your Groups
Create Adverts
Advertising on Facebook
Activity Log
News Feed Preferences
Settings
Log out
See less
Log out of all sessions
Edit

Security and login

We've reorganised a few things. Legacy contacts and the account deactivation optio
General

Recommended

Choose friends to contact if you are locked out
Nominate 3 to 5 friends to help if you are locked out of your account. We recommend this to every

Where you're logged in

Windows PC · Lowestoft, United Kingdom
Firefox · Active now

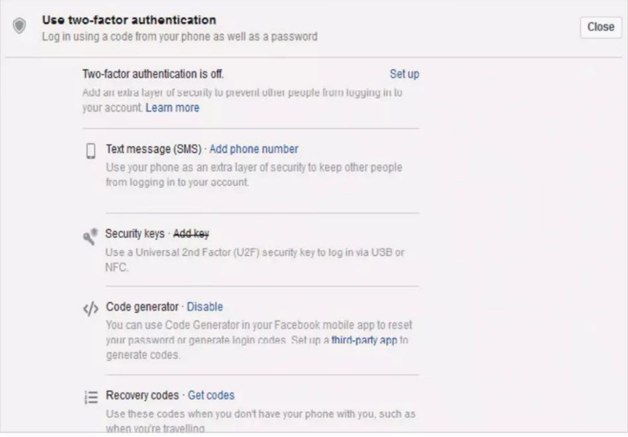
Android · Lowestoft, United Kingdom
Samsung Browser · 11 July at 14:45

Android · Lowestoft, United Kingdom
Android · 4 July at 12:02

Login

Change password
It's a good idea to use a strong password that you don't use elsewhere

In the same section, you're also able to set up two-factor authentication, utilising your phone, where Facebook will send a code to login with along with using your password. This elevated level of security ensures a higher degree of safety, as your account will be extremely difficult to hack.


Close
Set up
Learn more
Add phone number
Disable
third-party app
Get codes

Use two-factor authentication
Log in using a code from your phone as well as a password

Two-factor authentication is off.
Add an extra layer of security to prevent other people from logging in to your account.

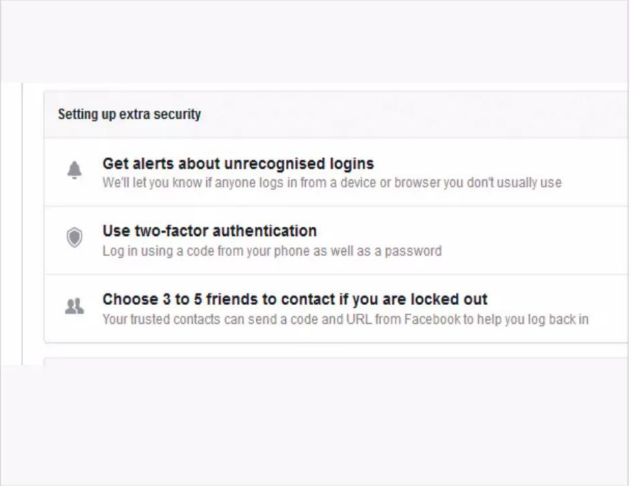
Text message (SMS) · Add phone number
Use your phone as an extra layer of security to keep other people from logging in to your account.

Security keys · ~~Add key~~
Use a Universal 2nd Factor (U2F) security key to log in via USB or NFC.

Code generator · Disable
You can use Code Generator in your Facebook mobile app to reset your password or generate login codes. Set up a third-party app to generate codes.

Recovery codes · Get codes
Use these codes when you don't have your phone with you, such as when you're travelling

Whilst in the Security and login page, click the 'Get alerts about unrecognised logins' section's Edit box, this enables you to view if your account is logged in from an unrecognised device. This particular function is handy to keep track of when and where your Facebook account is being used.



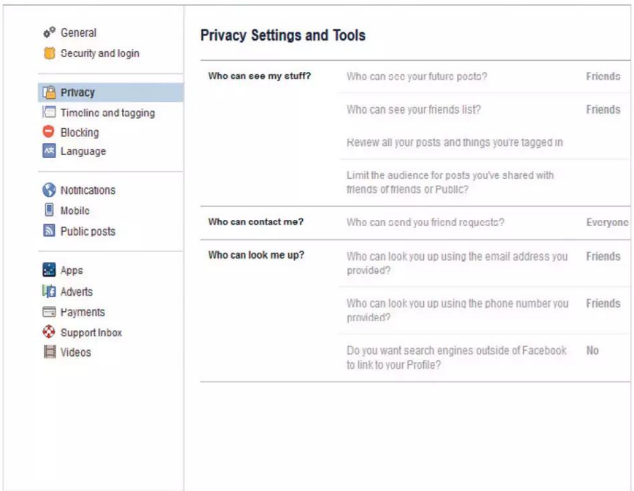
Setting up extra security

Get alerts about unrecognised logins
We'll let you know if anyone logs in from a device or browser you don't usually use

Use two-factor authentication
Log in using a code from your phone as well as a password

Choose 3 to 5 friends to contact if you are locked out
Your trusted contacts can send a code and URL from Facebook to help you log back in

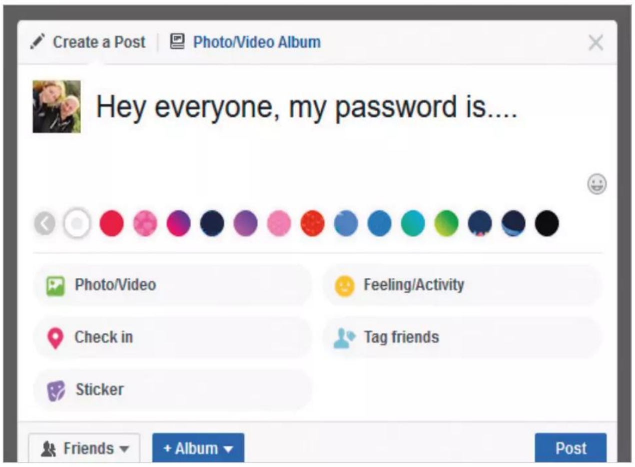
Click on the next section heading on the left-hand pane, Privacy. Take a moment to run through each of the options in this page, to ensure that your account is as private as possible, whilst still being available for true friends and family to add you to their friends lists.


General
Security and login
Privacy
Timeline and tagging
Blocking
Language
Notifications
Mobile
Public posts
Apps
Adverts
Payments
Support Inbox
Videos

Privacy Settings and Tools

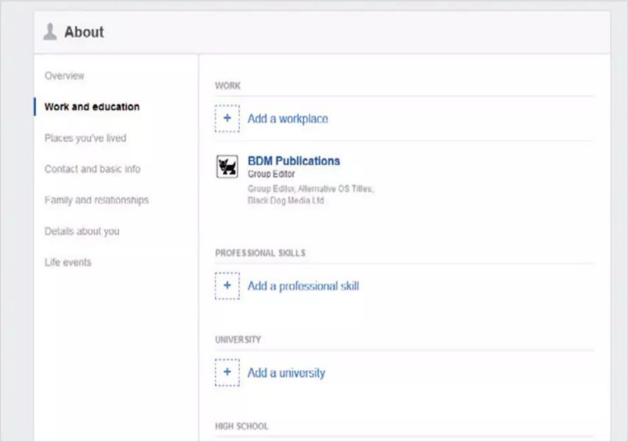
Who can see my stuff?	Who can see your future posts?	Friends
	Who can see your friends list?	Friends
	Review all your posts and things you're tagged in	
	Limit the audience for posts you've shared with friends of friends or Public?	
Who can contact me?	Who can send you friend requests?	Everyone
Who can look me up?	Who can look you up using the email address you provided?	Friends
	Who can look you up using the phone number you provided?	Friends
	Do you want search engines outside of Facebook to link to your Profile?	No

We're sure you don't need telling this, but never type your password into your Timeline. It may sound like a very basic tip but there have been instances of users being fooled, or simply not thinking of what they're doing or where they're typing, into entering their password into the Facebook Timeline.


Hey everyone, my password is....
Create a Post
Photo/Video Album
Photo/Video
Feeling/Activity
Check in
Tag friends
Sticker
Friends
+ Album
Post

Never accept a friend request from a random stranger. Sometimes they accompany their request with a message, something along the lines of 'hey, remember me? We met in town…', or something similar. The hope is that you'll accept the request blindly and once in your friend list, they can get all manner of details from you.

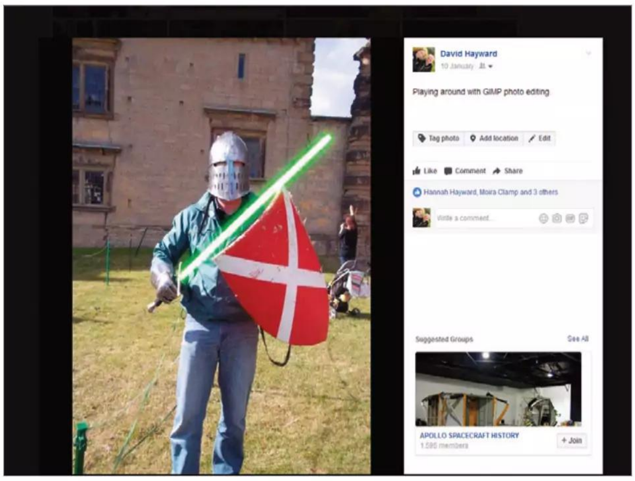
Although it's nice to put forward information about yourself in your Facebook account, be a little cautious and consider not entering too many details. It's very easy for someone to then retrieve information regarding your date of birth, where you live, where you went to school, where you work and so on.


BDM Publications
Group Editor
Group Editor, Alternative OS Titles, Black Dog Media Ltd
About
Overview
Work and education
Places you've lived
Contact and basic info
Family and relationships
Details about you
Life events
WORK
Add a workplace
PROFESSIONAL SKILLS
Add a professional skill
UNIVERSITY
Add a university
HIGH SCHOOL

Try to avoid being drawn into mass phishing posts, where the response asking is along the lines of 'List five things about yourself, then pass it on', or even posts that ask for likes. These are generated to catch active user accounts, which can then be used for phishing attempts.

Don't be fooled into thinking that posts asking for people to help locate a missing child, pet or object are real. Not only are most of these phishing attempts but often they can be attempts of someone trying to find a person; there could be a reason that the person in question has left, an abusive relationship perhaps.

Always think before you enter a post or reply to one. Just as you would in life, sometimes it's best not to say anything at all rather than offend or anger someone who's is blatantly baiting others. Think also about what images you post. Could your address or other details be discovered from the image?


David Hayward
10 January
Playing around with GIMP photo editing
Hannah Hayward, Moira Clamp and 3 others
Tag photo
Add location
Edit
Like
Comment
Share
Write a comment...
Suggested Groups
See All
APOLLO SPACECRAFT HISTORY
+ Join

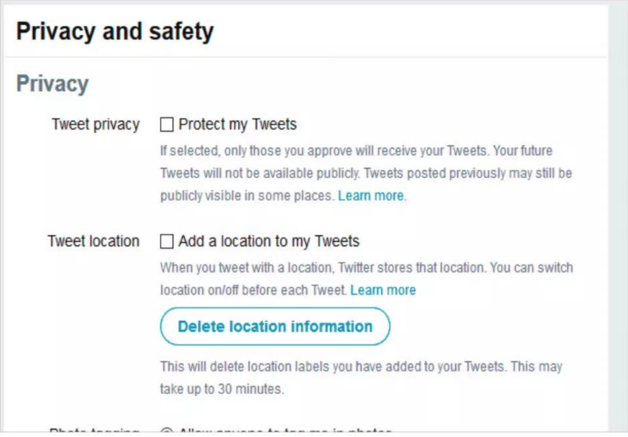
Staying Safe with Twitter for Teens

Twitter has been seen as both a force for good, allowing users from other parts of the world to communicate with what's going on in their country and as a platform for the nastier side of humanity. For teens, there's a lot to consider with staying safe on Twitter.

Twitter Twits

The age for setting up a Twitter account is thirteen but even adults can find themselves in a pickle from an errant Tweet or a Twitter-based phishing scam. Here are ten tips to help keep you safe on Twitter.

In Twitter, click on your profile picture and choose Settings and Privacy from the menu. To the left-side of the Twitter interface, click on the Privacy and safety link. Consider enabling Tweet Privacy and disabling Discoverability for improved safety.



Privacy and safety

Privacy

Tweet privacy ☐ Protect my Tweets

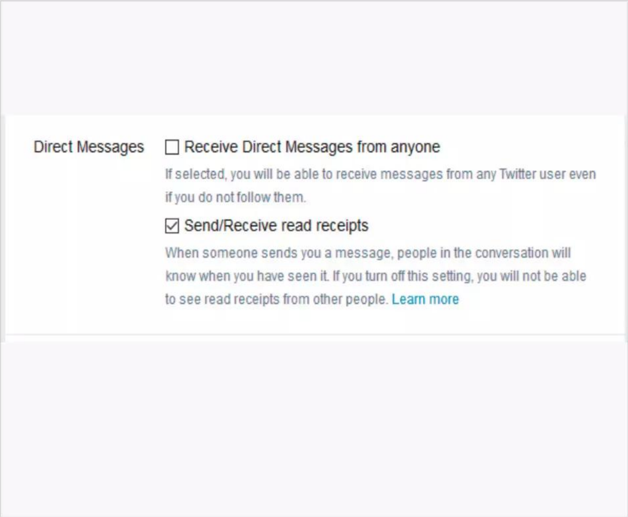
If selected, only those you approve will receive your Tweets. Your future Tweets will not be available publicly. Tweets posted previously may still be publicly visible in some places. Learn more.

Tweet location ☐ Add a location to my Tweets

When you tweet with a location, Twitter stores that location. You can switch location on/off before each Tweet. Learn more

This will delete location labels you have added to your Tweets. This may take up to 30 minutes.

Further down the Privacy and safety section, make sure that the Direct Messages option, Receive Direct Messages From Anyone is unticked. This way you won't get messages from anyone on Twitter, just those who you follow.



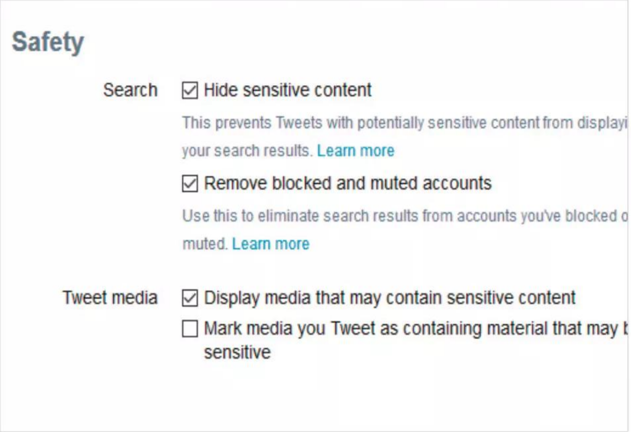
Direct Messages ☐ Receive Direct Messages from anyone

If selected, you will be able to receive messages from any Twitter user even if you do not follow them.

☑ Send/Receive read receipts

When someone sends you a message, people in the conversation will know when you have seen it. If you turn off this setting, you will not be able to see read receipts from other people. Learn more

Just under the Direct Messages options, look to the Safety section. Here you can opt whether to hide Tweets that may contain sensitive content, remove blocked or muted accounts or display media that may also contain sensitive content.



Safety

Search ☑ Hide sensitive content

This prevents Tweets with potentially sensitive content from displayi

your search results. Learn more

☑ Remove blocked and muted accounts

Use this to eliminate search results from accounts you've blocked o

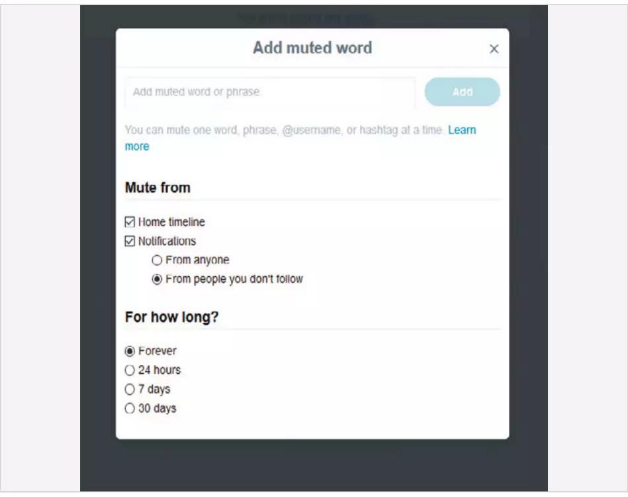
muted. Learn more

Tweet media ☑ Display media that may contain sensitive content

☐ Mark media you Tweet as containing material that may b

sensitive

To the left-hand options pane, click on the Muted Words section. With this option you're able to hide certain words, phrases, usernames or hash tags. This is a great option to mass block any content you never want to see, or that contains inappropriate content.



Add muted word

You can mute one word, phrase, @username, or hashtag at a time. Learn more

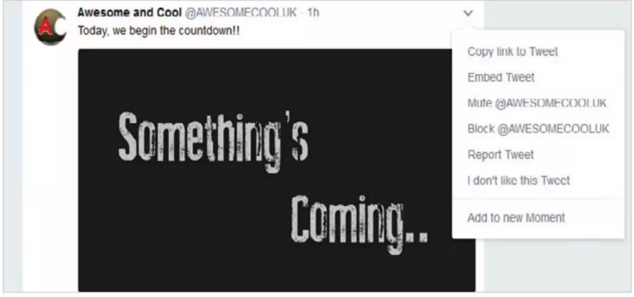
Mute from

☑ Home timeline
☑ Notifications
○ From anyone
● From people you don't follow

For how long?

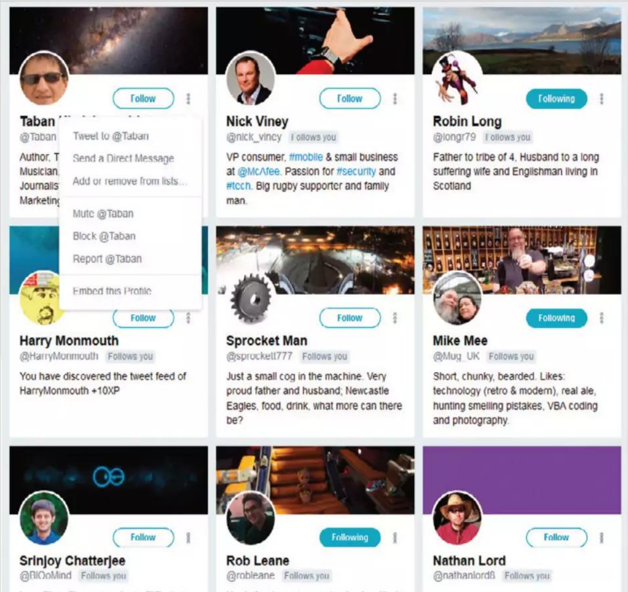
● Forever
○ 24 hours
○ 7 days
○ 30 days

If you see a Tweet from a user you don't like the look of, or is offensive in some way or form, you have several options available to you. Click the down-arrow next to the user's name and you can Mute, Block, Report or simply opt for I Don't Like This Tweet.


Awesome and Cool @AWESOMECOOLUK · 1h
Today, we begin the countdown!!

Something's
Coming..
Copy link to Tweet
Embed Tweet
Mute @AWESOMECOOLUK
Block @AWESOMECOOLUK
Report Tweet
I don't like this Tweet
Add to new Moment

As a Twitter user who hasn't enabled privacy, you're open to anyone finding and following you. You get an update as soon as someone does follow you and you then have the option to Mute, Block, Report or remove the user. Don't be afraid to remove a user if you don't know or trust them.


Taban
@Taban
Author, T
Musician
Journalis
Marketin

Nick Viney
@nick_viney Follows you
VP consumer, #mobile & small business at @McAfee. Passion for #security and #tech. Big rugby supporter and family man.

Robin Long
@longr79 Follows you
Father to tribe of 4. Husband to a long suffering wife and Englishman living in Scotland

Harry Monmouth
@HarryMonmouth Follows you
You have discovered the tweet feed of HarryMonmouth +10XP

Sprocket Man
@sprockett777 Follows you
Just a small cog in the machine. Very proud father and husband; Newcastle Eagles, food, drink, what more can there be?

Mike Mee
@Mug_UK Follows you
Short, chunky, bearded. Likes: technology (retro & modem), real ale, hunting smelling pistakes, VBA coding and photography.

Srinjoy Chatterjee
@BlOoMind Follows you

Rob Leane
@robleane Follows you

Nathan Lord
@nathanlord8 Follows you

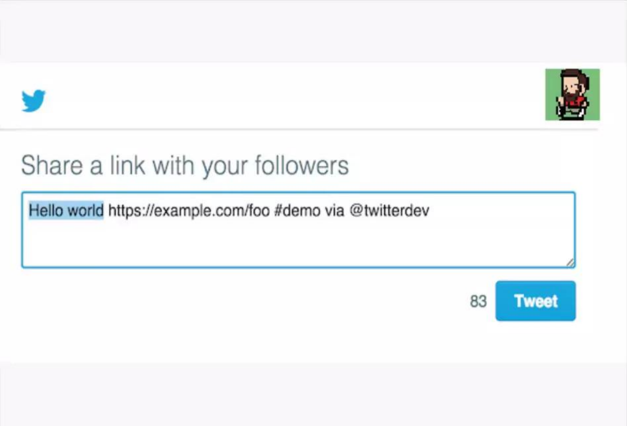
Follow
Following
Tweet to @Taban
Send a Direct Message
Add or remove from lists...
Mute @Taban
Block @Taban
Report @Taban
Embed this Profile

Just as with Facebook posts, don't be fooled into commenting on posts that are phishing attempts. These are created to farm for active accounts and gather information about users' tweets, and any personal details.

Try not to reply to any Direct Messages sent to you on Twitter. Whilst some messages and accounts are real, perhaps a job offer for example, many are simply Twitter bots phishing for active accounts and details.

DIRECT
MESSAGES

Never click on any links that appear in a Tweet or as part of a Direct Message. Unless you specifically know the user and can trust their Tweets or messages; the link may lead you to a site that's riddled with malware or further scams.


Share a link with your followers

Hello world https://example.com/foo #demo via @twitterdev

Always think before you reply to any Tweets, post your own or upload any images. It's very easy to offend and become involved in a heated war over something you don't want to be a part of. Don't become the victim of anyone baiting you into an argument. If you are, then sign off and leave the group.

twitter
Search
What's happenin

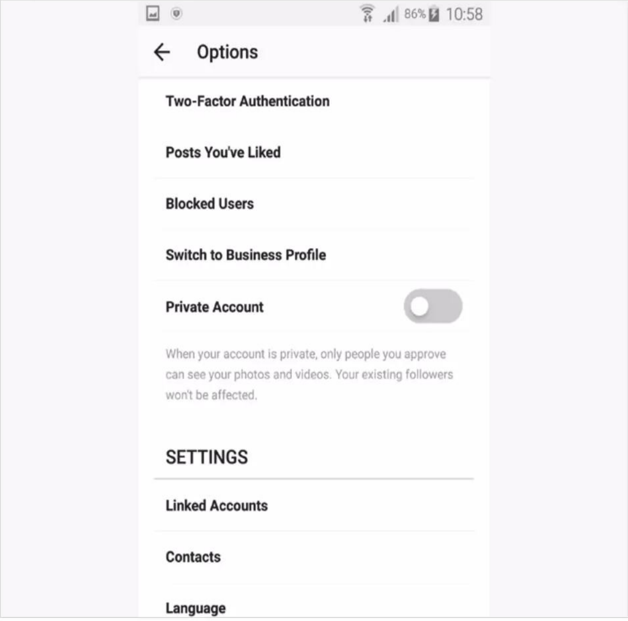
Staying Safe with Instagram for Teens

Much of today's Internet youth has moved from Facebook and now inhabits Instagram. This social media platform is used by celebrities, politicians and a user base of over 700 million. Needless to say, it's population is varied and contains those who you wouldn't want contacting you.

Insta-scam

In compliance with the Children's Online Privacy Protection Act, Instagram requires that its users' minimum age to sign up is 13 but even as a young teen, there's still plenty to do to help improve your safety.

Instagram is a simple photo and sharing app but there's plenty of material and content out there that shouldn't be viewed by minors. That being the case, tap the person (profile) icon in the bottom right, then the three vertical dots in the top right. This opens the Instagram Options window. From there, scroll down and enable Private Account.



86% 10:58

Options

Two-Factor Authentication

Posts You've Liked

Blocked Users

Switch to Business Profile

Private Account ○

When your account is private, only people you approve can see your photos and videos. Your existing followers won't be affected.

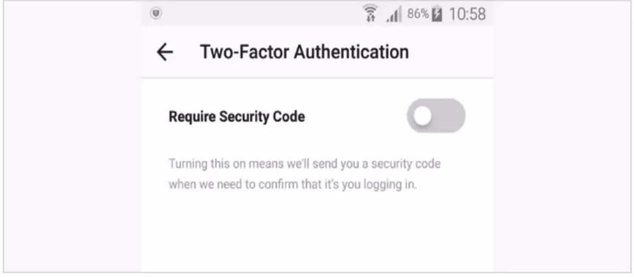
SETTINGS

Linked Accounts

Contacts

Language

Private Accounts are visible, but not the content you've posted. Anyone who wants to follow you will need to send a request, so you can easily decline any users. Whilst still in the Account section, scroll up and consider enabling Two-Factor Authentication, for additional security.



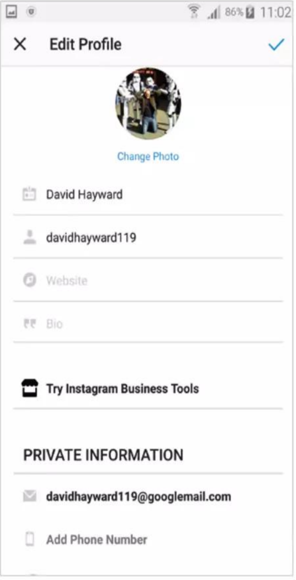
86% 10:58

Two-Factor Authentication

Require Security Code ○

Turning this on means we'll send you a security code when we need to confirm that it's you logging in.

Staying in the Account section, tap on Edit Profile. This is where you can create a profile picture and include other information about yourself. It's up to you how much info you want to add but it's often best to take a secure-minded approach and not give away too much.



86% 11:02

Edit Profile ✓

Change Photo

David Hayward

davidhayward119

Website

Bio

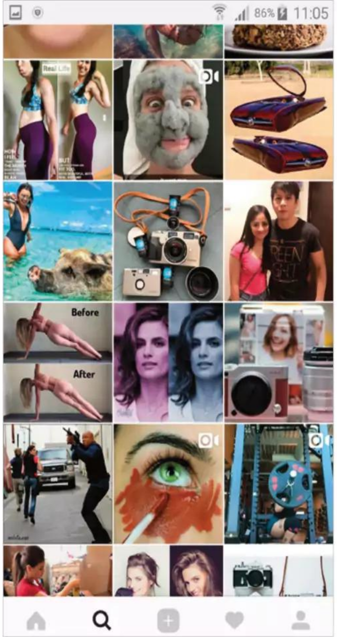
Try Instagram Business Tools

PRIVATE INFORMATION

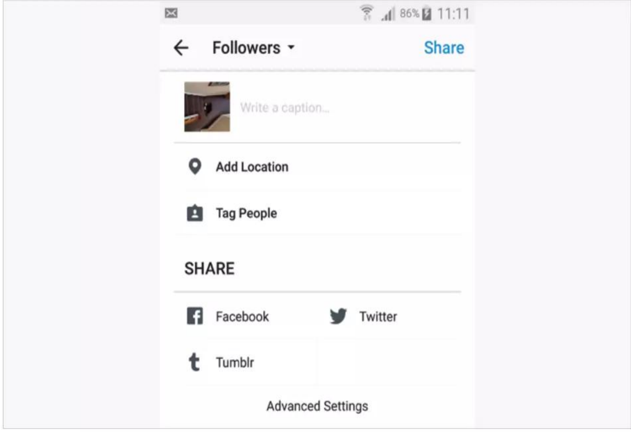
davidhayward119@googlemail.com

Add Phone Number

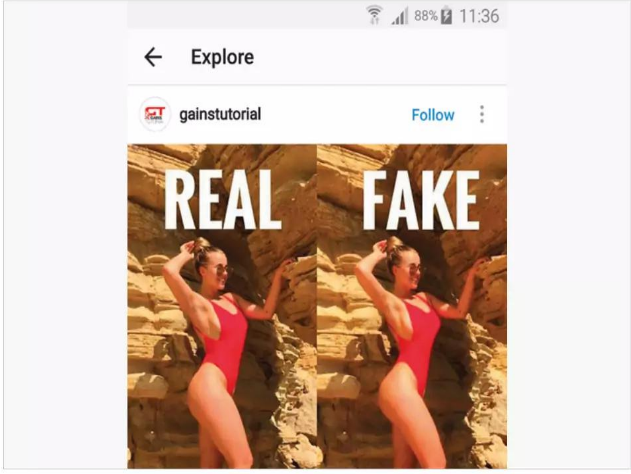
The magnifying glass icon is the Instagram search function. It often displays images and videos based on your likes and who you follow, such as amazing landscapes but it's also known to insert content that isn't always appropriate for younger viewers. Don't open the image, even to report it, it's best to just ignore it.



Uploading an image provides multiple options, from choosing a filter, image style and so on, to tagging other people, sharing with other social media platforms and adding a location. It may seem harmless enough but consider not sharing your location, as it's instantly available on Instagram. It doesn't take a genius to locate where you are.

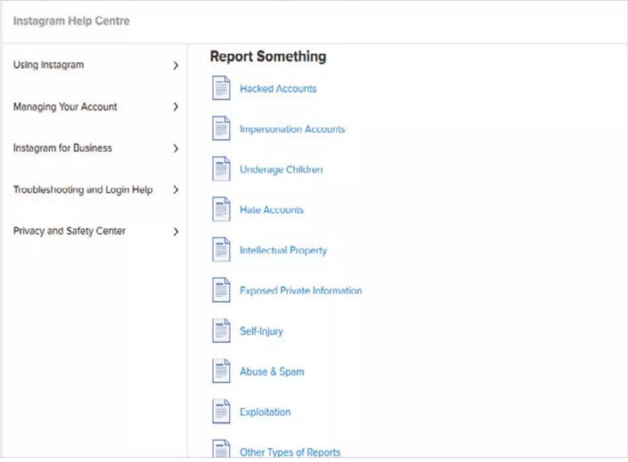


Be wary of what you see on Instagram. This applies to other social media platforms too but Instagram users appear to revel in posting fake or photoshopped images of themselves or others, or even events. It's a huge source of image-aware and body-conscious behaviour, that's influential to younger minds. In short, don't always believe what you see on Instagram.



If you've approved a user, whilst in privacy mode, and they start to send you inappropriate images, video or comments, then make sure that you show a parent or guardian. Don't respond to the sender and don't unfollow or block them until you've shown someone or taken a screenshot of the content.

The Instagram Help Centre is where you can report a user for inappropriate content, abuse, spam, hacked accounts or exposure of private information. It's available from any browser, as well as from the app itself. Be familiar with it, as you may need it someday.



Instagram Help Centre

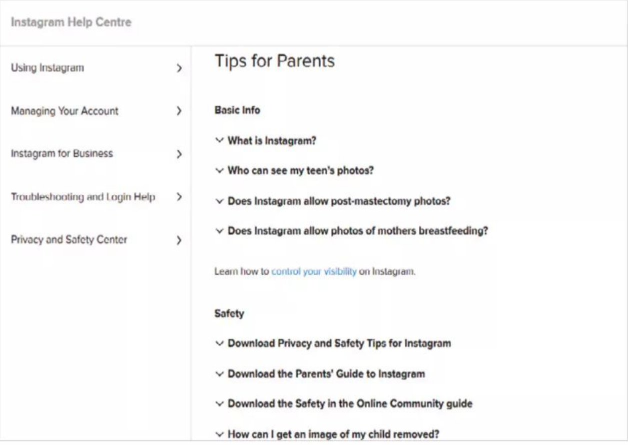
- Using Instagram
- Managing Your Account
- Instagram for Business
- Troubleshooting and Login Help
- Privacy and Safety Center

Report Something

- Hacked Accounts
- Impersonation Accounts
- Underage Children
- Hate Accounts
- Intellectual Property
- Exposed Private Information
- Self-Injury
- Abuse & Spam
- Exploitation
- Other Types of Reports

If you find yourself involved with someone or a group of people who are obviously trying to create some form of hate messaging, bullying or similar, make sure you take any screenshots as proof (in case someone reports the incident) and walk away from the conversation. Block accounts if necessary, to stop further instances happening.

Parents: before you allow your young teen access to Instagram, it's best you have a read through the company's Tips for Parents section. This can be found at **https://help.instagram**.com/154475974694511/?helpref=hc_fnav and includes everything you need to know about what it is and how it works.



Instagram Help Centre

- Using Instagram
- Managing Your Account
- Instagram for Business
- Troubleshooting and Login Help
- Privacy and Safety Center

Tips for Parents

Basic Info

- What is Instagram?
- Who can see my teen's photos?
- Does Instagram allow post-mastectomy photos?
- Does Instagram allow photos of mothers breastfeeding?

Learn how to control your visibility on Instagram.

Safety

- Download Privacy and Safety Tips for Instagram
- Download the Parents' Guide to Instagram
- Download the Safety in the Online Community guide
- How can I get an image of my child removed?

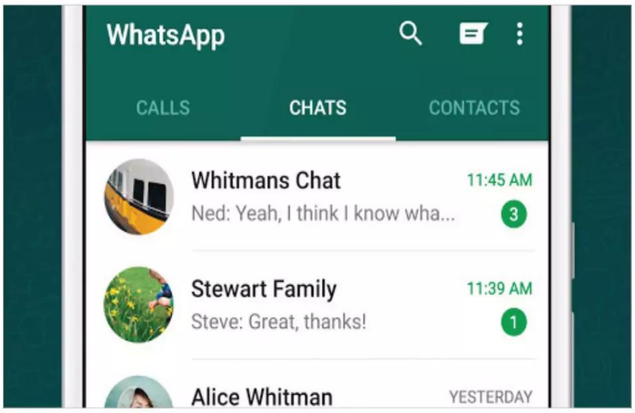
Staying Safe with WhatsApp for Teens

WhatsApp is a free messenger app that can make Internet voice and video calls, send messages, images and other content. It's a little safer than some social media platforms, as you need a user's phone number before being able to add them; but there's always room for further security.

What App?

There's plenty you can do to improve your privacy and security and remain safe when using WhatsApp. Here are ten tips for teens and parents when using this popular app.

According to WhatsApp's terms, the minimum age needed is thirteen years old before a young person is allowed to use the service. Thankfully young teens are only able to contact those who they have added to their WhatsApp account but it's best to occasionally check their contact list in case of someone unknown being added.

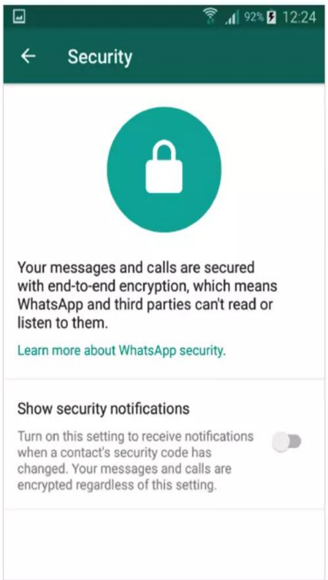


Whitmans Chat 11:45 AM
Ned: Yeah, I think I know wha... 3

Stewart Family 11:39 AM
Steve: Great, thanks! 1

Alice Whitman YESTERDAY

WhatsApp has a high-degree of encryption and security already built-in; however, by tapping the Security option within the Account option, you're able to display any security notifications that may crop up from time to time.



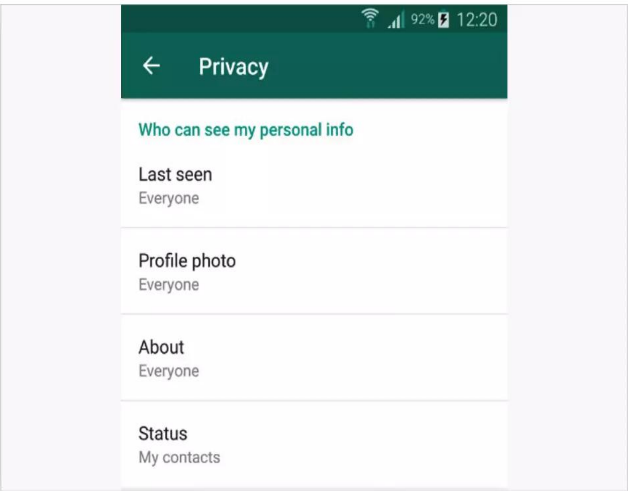
Your messages and calls are secured with end-to-end encryption, which means WhatsApp and third parties can't read or listen to them.

Learn more about WhatsApp security.

Show security notifications

Turn on this setting to receive notifications when a contact's security code has changed. Your messages and calls are encrypted regardless of this setting.

Tap the three vertical dots in the top right of the WhatsApp interface, followed by tapping the Settings option. Now tap the Account option, then Privacy. In here you're able to limit the amount of personal information a contact can view, as well as block any contacts.



Who can see my personal info

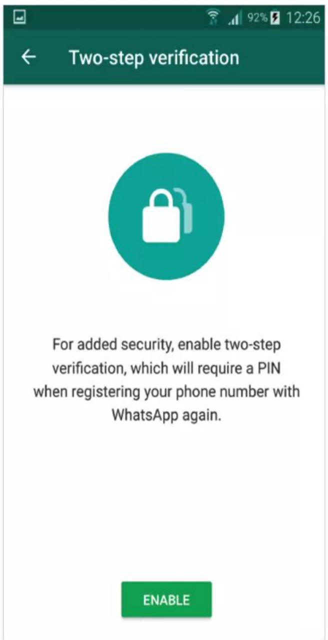
Last seen
Everyone

Profile photo
Everyone

About
Everyone

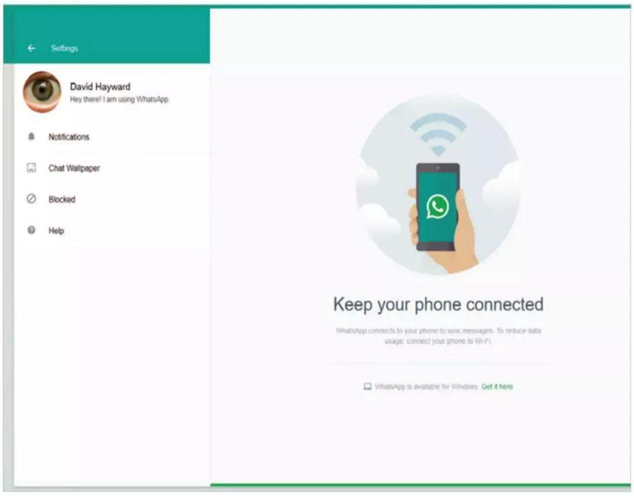
Status
My contacts

Again, from the Account option, tap on the Two-Step Verification setting to set up a PIN in addition to your usual login information. This will enhance the security of your WhatsApp account, should you ever lose your device.



For added security, enable two-step verification, which will require a PIN when registering your phone number with WhatsApp again.

If you're using the web version of WhatsApp, click on the three vertical dots, followed by Settings. Although not as comprehensive as the app's settings, you can set up your notifications and block any users if necessary.


Settings
Notifications
Chat Wallpaper
Blocked
Help
Get it here

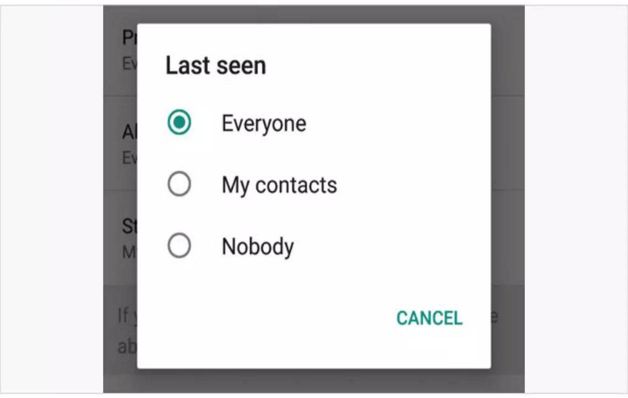
David Hayward
Hey there! I am using WhatsApp.

Keep your phone connected

WhatsApp connects to your phone to sync messages. To reduce data usage, connect your phone to Wi-Fi.

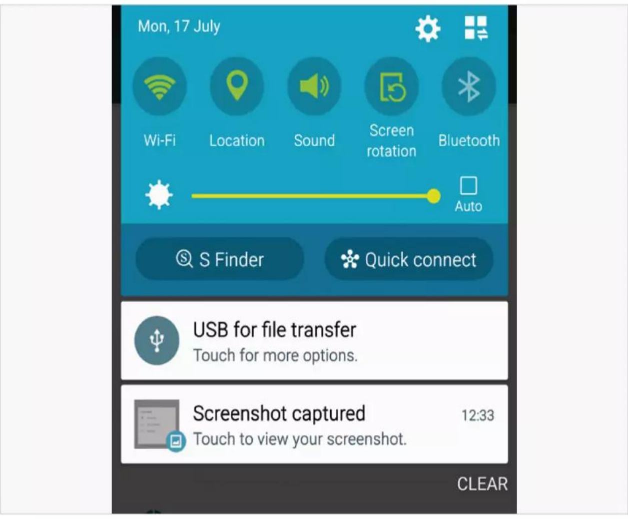
WhatsApp is available for Windows. Get it here

Back to the Privacy settings in the app's Account option, don't forget to limit the Last Seen setting. The three options available are: Everyone, My Contacts and Nobody. This will prevent contacts from seeing where you were when you posted any content.



Last seen
● Everyone
○ My contacts
○ Nobody

WhatsApp also utilises the device's built-in Location feature. This enables geo-tagging of content as it's uploaded. If you want to upload something but want to make sure that nobody knows where you are, quickly tap the Location function on your device to disable it before uploading.


Mon, 17 July
Wi-Fi
Location
Sound
Screen rotation
Bluetooth
Auto
S Finder
Quick connect
CLEAR

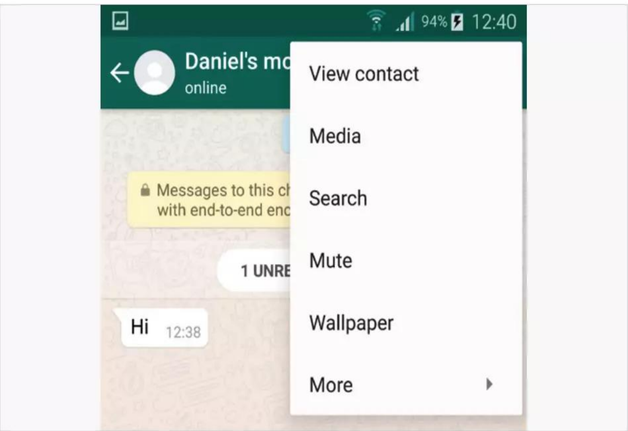
USB for file transfer
Touch for more options.

Screenshot captured 12:33
Touch to view your screenshot.

If someone becomes aggressive or starts to bully you in WhatsApp, take a screenshot and record the evidence, then approach a parent and guardian and show them what's going on. Don't respond to the person and don't block them immediately. Always talk to a parent or guardian before doing anything.

CYBER
BULLYING

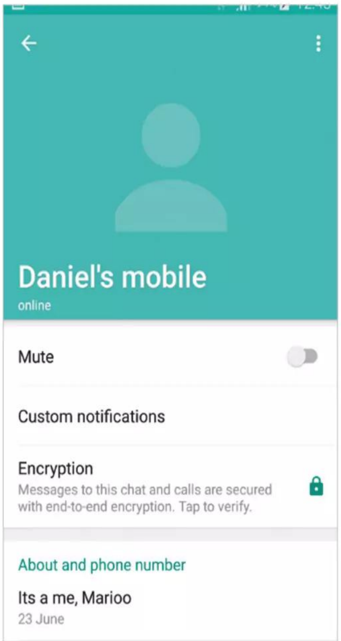
Any contacts that send you a message can be blocked, muted and the chat content cleared or emailed if needed. Just open the message, tap the three vertical dots and select the appropriate option from the menu.


94% 12:40
Daniel's mo
online
View contact
Media
Search
Mute
Wallpaper
More
1 UNRE

Messages to this ch
with end-to-end enc

Hi 12:38

Once you have a message open, long tap the contact and you can see the contact's information. From there you're able to block them, report them as a spam user, mute them or even verify that the messages sent are fully encrypted.


Daniel's mobile
online
Mute
Custom notifications
Encryption
About and phone number

Messages to this chat and calls are secured with end-to-end encryption. Tap to verify.

Its a me, Marioo
23 June

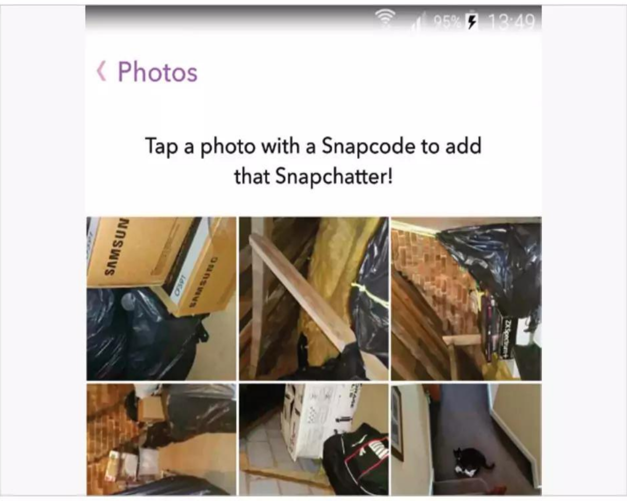
Staying Safe with Snapchat for Teens

Popular amongst young teens, Snapchat has continually raised its appeal by offering alluring features at the cost of security and privacy. The most recent update (at the time of writing) is Snap Maps, a feature that tells everyone where you currently are.

Safety Snaps

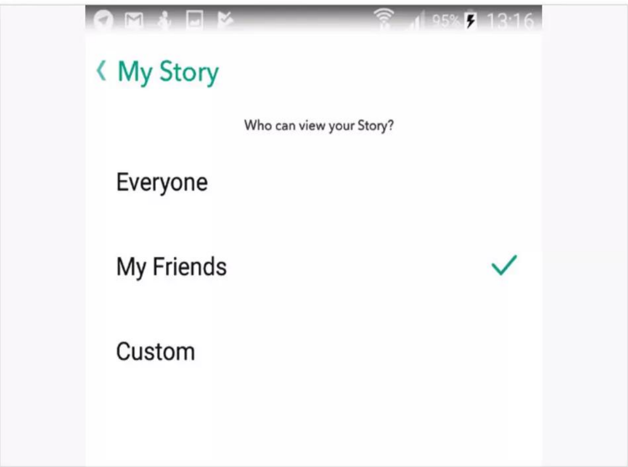
Snapchat has some useful features but also some slightly scary security issues. It's best then to make sure that you're as safe as possible when using it.

Parents: Take the time to look through your child's Snapchat contacts. Together you can limit who can see what and who can contact your child through Snapchat's various functions.


95% 13:49
‹ Photos

Tap a photo with a Snapcode to add that Snapchatter!

You can create your own Snapchat Stories, by tapping the three dots in a triangle in the bottom right of the Snapchat interface. Make sure that you also tap the cog icon in the top right within Stories, in here you'll be able to limit who sees your stories. Try and avoid choosing Everyone, if possible.


95% 13:16
‹ My Story

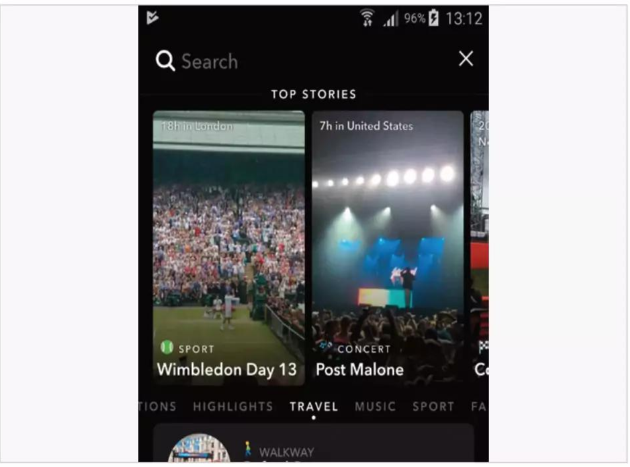
Who can view your Story?

Everyone

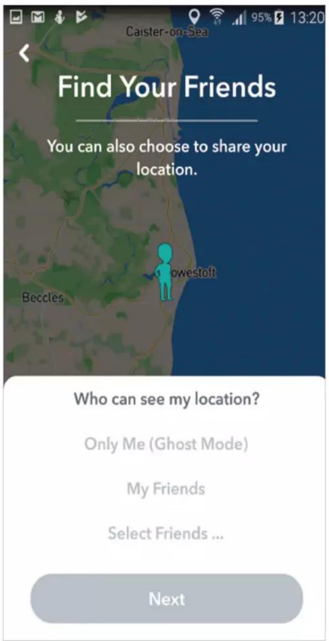
My Friends ✓

Custom

Tapping the magnifying glass icon will open the global Snapchat Top Stories. From there a user can search for something specific or view any Snapchats via the various headings. Be careful here, there's a lot of inappropriate content out there, along with dubious individuals who would like your information.


96% 13:12
Search
TOP STORIES
18h in London
7h in United States
SPORT
Wimbledon Day 13
CONCERT
Post Malone
IONS HIGHLIGHTS TRAVEL MUSIC SPORT FA
WALKWAY

Snap Maps is the newest feature to Snapchat, one that enables other Snapchat users to see where you are in the world. To open it, pinch your fingers like you're zooming out from the camera screen. When asked, you're able to set who can see your location. Always ensure you know your friends, or enable Ghost mode for better privacy.


95% 13:20
Caister-on-Sea
Lowestoft
Beccles

Find Your Friends

You can also choose to share your location.

Who can see my location?

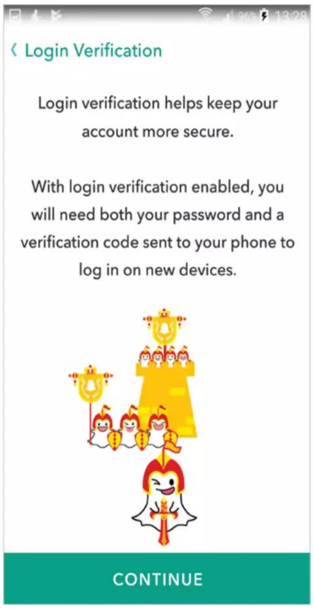
Only Me (Ghost Mode)

My Friends

Select Friends ...

Next

Tap on the Snapchat icon, followed by the cog in the top right to access your account settings. Scroll down a little way to Login Verification and tap it. This is a two-step authentication process that requires both a code sent to your device, as well as your login details to open Snapchat. Useful if you ever lose your device.



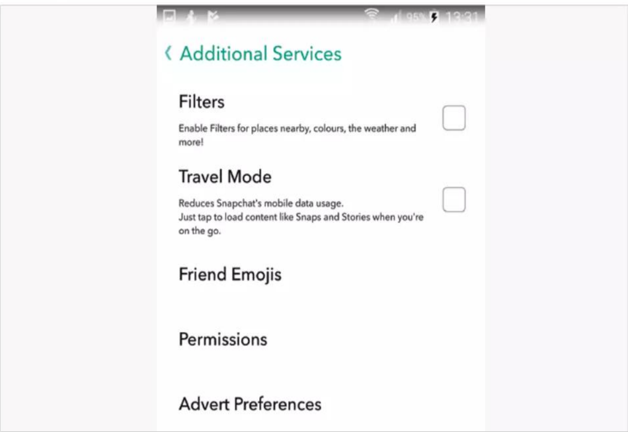
‹ Login Verification

Login verification helps keep your account more secure.

With login verification enabled, you will need both your password and a verification code sent to your phone to log in on new devices.

CONTINUE

Whilst still in the account settings, scroll down to Manage Preferences under the Additional Services heading. In here you can limit the mobile data use and enable filters for nearby places, change the app permissions and advert preferences.



‹ Additional Services

Filters ☐
Enable Filters for places nearby, colours, the weather and more!

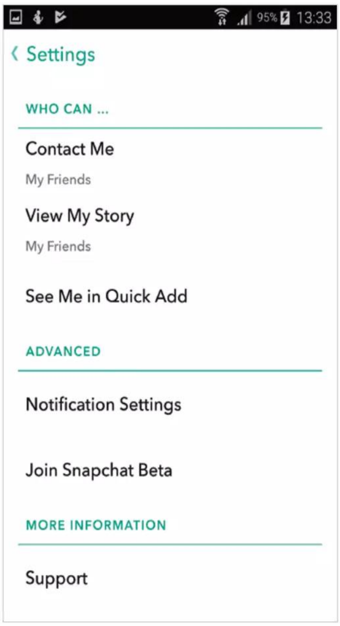
Travel Mode ☐
Reduces Snapchat's mobile data usage.
Just tap to load content like Snaps and Stories when you're on the go.

Friend Emojis

Permissions

Advert Preferences

Under the Additional Services heading, the Who Can… heading enables you to specify who can contact you or see your Stories. It's best to limit your account so only friends are able to see you or any posts you make, as opposed to the Everyone option.



95% 13:33

‹ Settings

WHO CAN ...

Contact Me
My Friends

View My Story
My Friends

See Me in Quick Add

ADVANCED

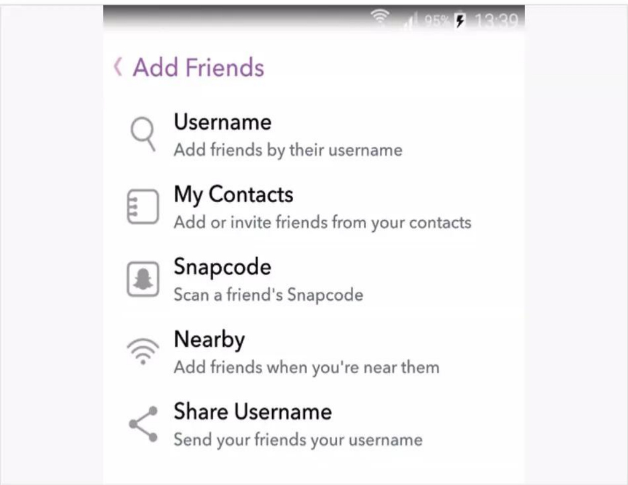
Notification Settings

Join Snapchat Beta

MORE INFORMATION

Support

Be wary of the Add Friends function in Snapchat. From it you can add friends in your contacts list, any that have sent you their Snapcode, shared friends lists, or you can opt to locate other Snapchat users based on whether they're nearby. Obviously this is a privacy and security concern, so be aware of it.



‹ Add Friends

Username
Add friends by their username

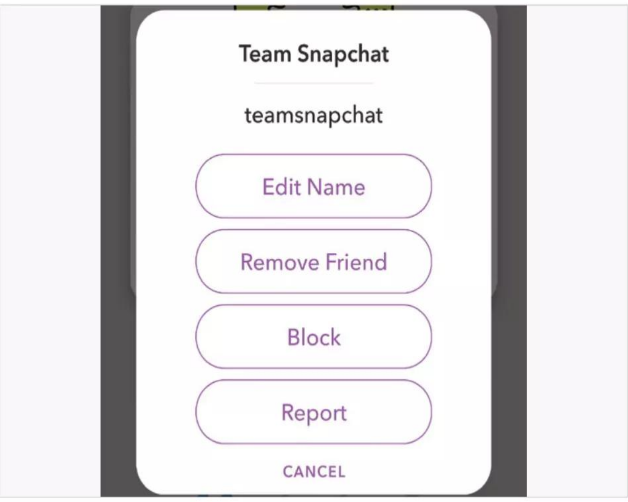
My Contacts
Add or invite friends from your contacts

Snapcode
Scan a friend's Snapcode

Nearby
Add friends when you're near them

Share Username
Send your friends your username

You can easily remove friends, block and report other Snapchat users by long pressing the contact or Snapchat feed and selecting the option from the menu. Make sure you've taken any screenshots of inappropriate content before blocking, to use as proof if reporting the contact.



Team Snapchat

teamsnapchat

Edit Name

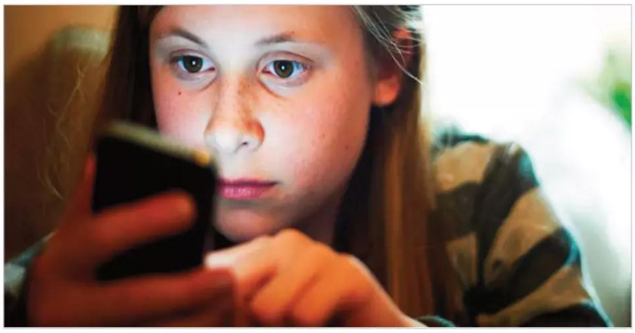
Remove Friend

Block

Report

CANCEL

Just as with all social media platforms, if you're uncomfortable with the content or messages that someone is sending you, tell a parent, guardian, teacher or other responsible adult. Don't respond, don't send anything to them and always think before posting any images of yourself and your location.



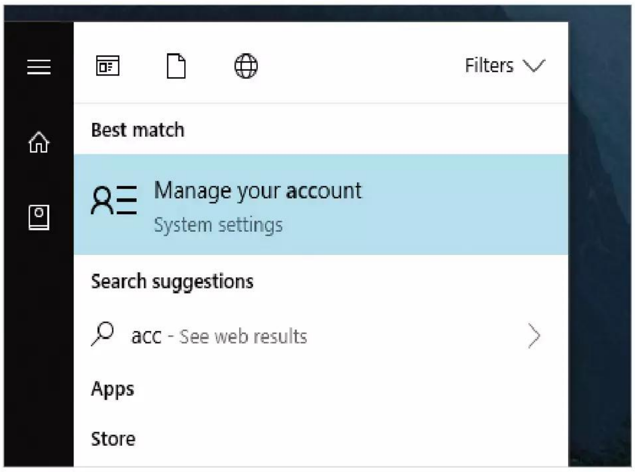
Creating a Child Account in Windows 10

If you're sharing a Windows 10 computer with your children, or they have one for themselves, then setting them up with their own account will work better for you both in the long run. A Windows 10 child's account gives them freedom, and you can set up certain restrictions.

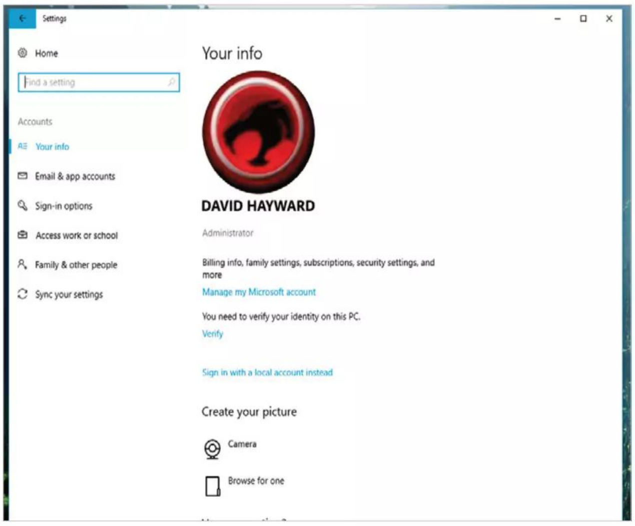
Windows 10 for Children

With a Windows 10 child account you're able to set up age restrictions, time limits and ensure they're not visiting sites or using apps they shouldn't.

STEP 1 Start off by clicking the Windows Start button and typing 'account'. The first result that should appear is Manage your account, if anything else appears, maybe you have some work labelled 'account', then scroll down until you find the Manage your account option.


Filters
Best match
Manage your account
System settings
Search suggestions
acc - See web results
Apps
Store

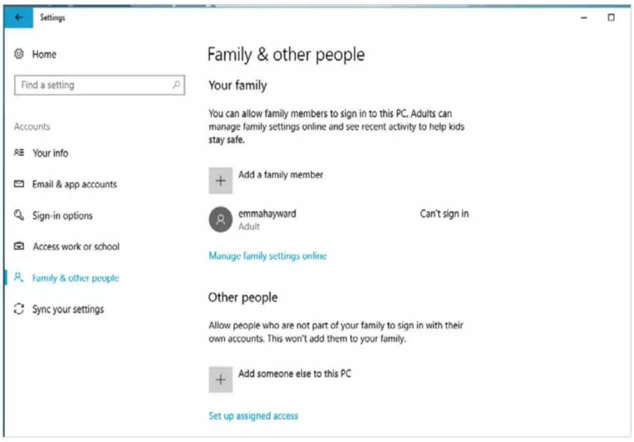
STEP 2 You now find yourself at the Windows 10 Settings page, in the Accounts section portal. Notice there are links down the left-hand side, look for the Family & Other People link and click it to continue with the process.


Settings
Home
Find a setting
Accounts
Your info
Email & app accounts
Sign-in options
Access work or school
Family & other people
Sync your settings
Your info
DAVID HAYWARD
Administrator
Manage my Microsoft account
Verify
Sign in with a local account instead
Create your picture
Camera
Browse for one

Billing info, family settings, subscriptions, security settings, and more

You need to verify your identity on this PC.

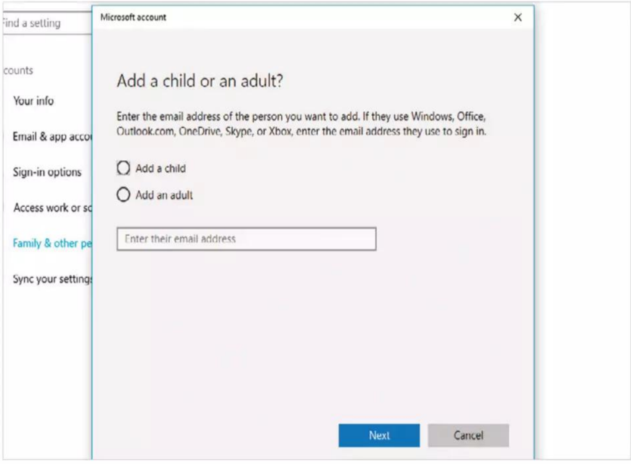
STEP 3 You need to sign in with a Microsoft account for this to work. If you've not already set up a main Microsoft login account for Windows, you'll need to click the Sign in with a Microsoft account option. Once done, you're presented with the current family members who already have MS accounts.


Settings
Home
Find a setting
Accounts
Your info
Email & app accounts
Sign-in options
Access work or school
Family & other people
Sync your settings
Family & other people
Your family
Add a family member
emmahayward
Adult
Can't sign in
Manage family settings online
Other people
Add someone else to this PC
Set up assigned access

You can allow family members to sign in to this PC. Adults can manage family settings online and see recent activity to help kids stay safe.

Allow people who are not part of your family to sign in with their own accounts. This won't add them to your family.

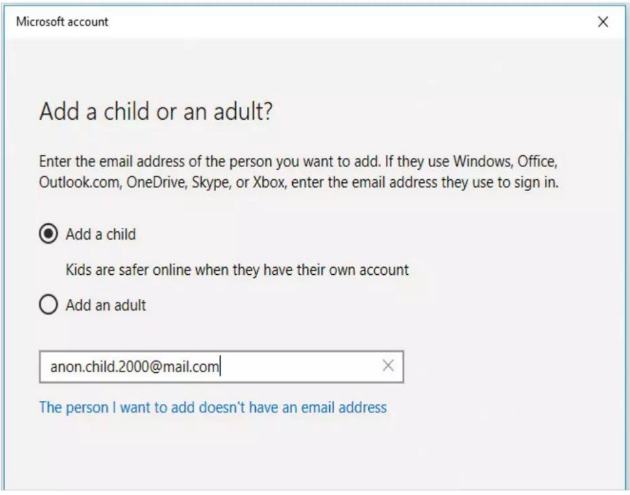
STEP 4 Next click on the Add a Family Member link, next to the plus sign under the Your Family section. This will launch a new pop-up window to create a new Microsoft account. You need to make sure that your child has an email address and that you or they currently have access to it to authenticate the process.


Microsoft account
Add a child or an adult?
Enter their email address
Next
Cancel

Enter the email address of the person you want to add. If they use Windows, Office, Outlook.com, OneDrive, Skype, or Xbox, enter the email address they use to sign in.

○ Add a child
○ Add an adult

STEP 5 Click the Add a Child option in the new account window and enter their email in the text box section below. When you're ready, click on the Next button.



Microsoft account

Add a child or an adult?

Enter the email address of the person you want to add. If they use Windows, Office, Outlook.com, OneDrive, Skype, or Xbox, enter the email address they use to sign in.

● Add a child

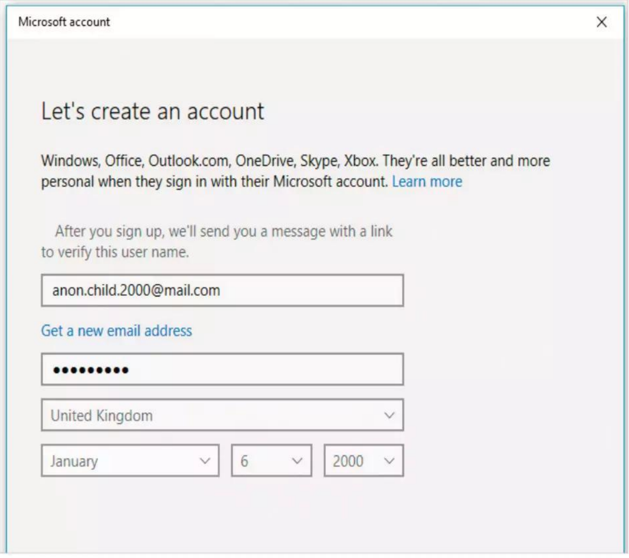
Kids are safer online when they have their own account

○ Add an adult

anon.child.2000@mail.com

The person I want to add doesn't have an email address

STEP 6 You now get the message that it's not a Microsoft account, click the link to Create a Microsoft Account. This will bring you to a new window with the email address you've entered already filled in. Complete the relevant details and click the Next button to continue.



Microsoft account

Let's create an account

Windows, Office, Outlook.com, OneDrive, Skype, Xbox. They're all better and more personal when they sign in with their Microsoft account. Learn more

After you sign up, we'll send you a message with a link to verify this user name.

anon.child.2000@mail.com

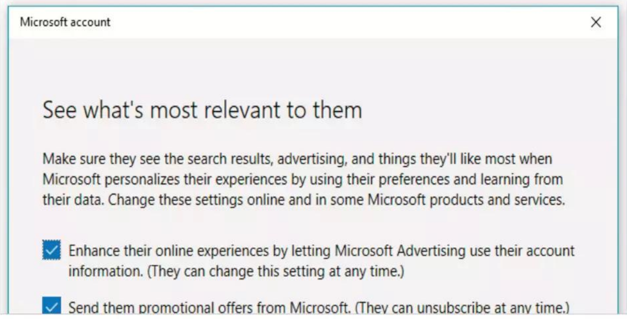
Get a new email address

•••••••••

United Kingdom

January 6 2000

STEP 7 The next section details what level of search and advertising Microsoft will allow to the account. Obviously you can untick both boxes or leave them as they are, it all depends on what you want. However, for the sake of enhanced privacy, we recommend unticking both. Click Next when you're ready.



Microsoft account

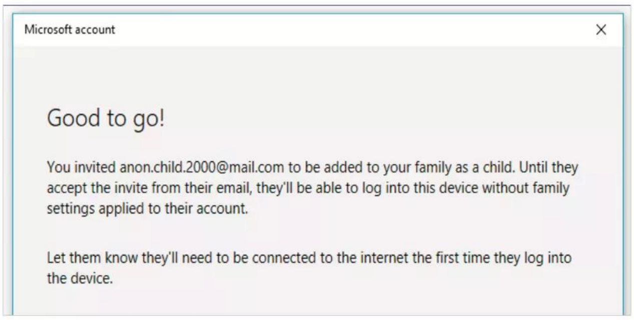
See what's most relevant to them

Make sure they see the search results, advertising, and things they'll like most when Microsoft personalizes their experiences by using their preferences and learning from their data. Change these settings online and in some Microsoft products and services.

☑ Enhance their online experiences by letting Microsoft Advertising use their account information. (They can change this setting at any time.)

☑ Send them promotional offers from Microsoft. (They can unsubscribe at any time.)

STEP 8 The child's account is now ready to be activated. The message box informs you that you need to respond to the email Microsoft has sent before they're able to login in to the Windows 10 computer. Click the Close button when you're ready.



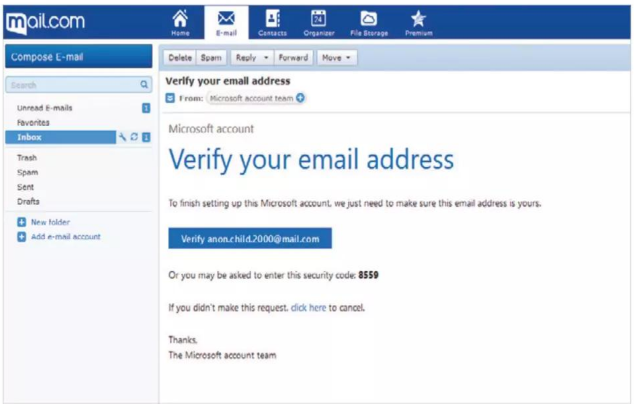
Microsoft account

Good to go!

You invited anon.child.2000@mail.com to be added to your family as a child. Until they accept the invite from their email, they'll be able to log into this device without family settings applied to their account.

Let them know they'll need to be connected to the internet the first time they log into the device.

STEP 9 Microsoft will send some emails to the child's account. One will be a Verification email, and you, or your child, will need to click the link to activate the account; they need to login to Microsoft online to complete the process. The other email will be an invitation to join the family account, which you also need to Accept.



Verify your email address

From: Microsoft account team

Microsoft account

Verify your email address

To finish setting up this Microsoft account, we just need to make sure this email address is yours.

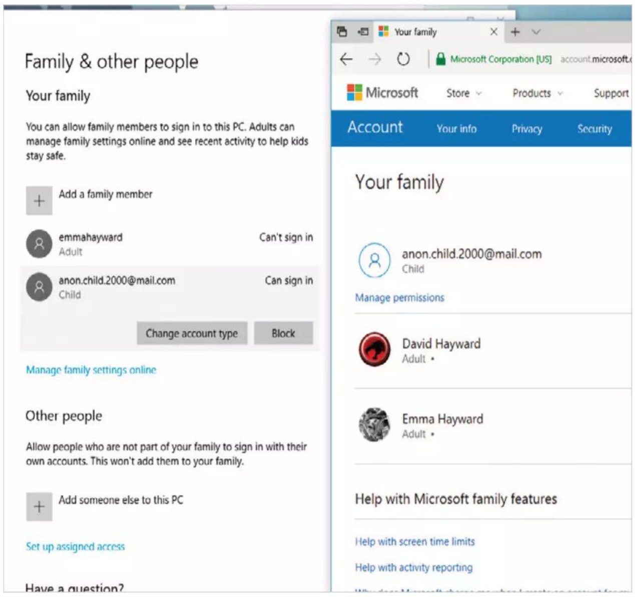
Verify anon.child.2000@mail.com

Or you may be asked to enter this security code: **8559**

If you didn't make this request, click here to cancel.

Thanks,
The Microsoft account team

STEP 10 Using the child account to join the family will send emails to you confirming the accepted invitation. Back at the Windows 10 Family & Other People window, you can now click the child's account and allow it to login, or manage it via the Microsoft Family portal online, which we'll look at in the next tutorial.



Family & other people

Your family

You can allow family members to sign in to this PC. Adults can manage family settings online and see recent activity to help kids stay safe.

Add a family member

emmahayward Adult — Can't sign in

anon.child.2000@mail.com Child — Can sign in

Change account type Block

Manage family settings online

Other people

Allow people who are not part of your family to sign in with their own accounts. This won't add them to your family.

Add someone else to this PC

Set up assigned access

Have a question?

Your family

anon.child.2000@mail.com Child

Manage permissions

David Hayward Adult

Emma Hayward Adult

Help with Microsoft family features

Help with screen time limits

Help with activity reporting

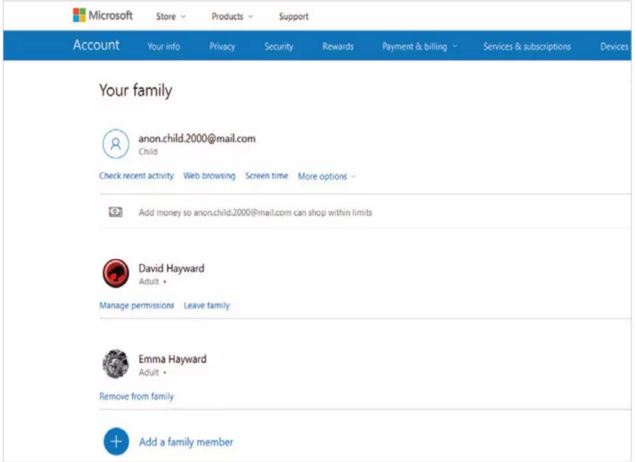
Windows 10 Family Features

Microsoft's Family portal is a continually updating service that allows you to monitor, control and share features across Windows machines and Xbox consoles. It's designed to help share calendars, set screen times for games and set up safe browsing.

Happy Families

The Microsoft Family portal is where you're able to set the various features. First, you need to browse to https://account.microsoft.com to login with your MS account.

STEP 1 When you've logged in to the Microsoft account online, click on the Family link found along the top set of menu options. This will display the current members of your Microsoft account, adults and any children you've added, as per the previous tutorial.


Microsoft
Store
Products
Support
Account
Your info
Privacy
Security
Rewards
Payment & billing
Services & subscriptions
Devices

Your family

anon.child.2000@mail.com
Child
Check recent activity Web browsing Screen time More options

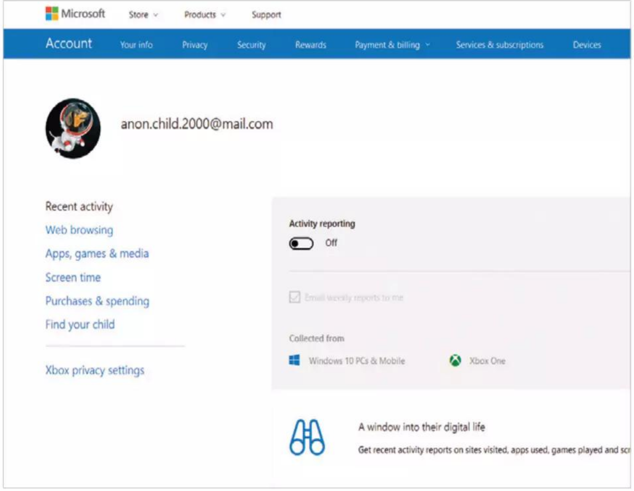
Add money so anon.child.2000@mail.com can shop within limits

David Hayward
Adult
Manage permissions Leave family

Emma Hayward
Adult
Remove from family

Add a family member

STEP 2 Under the child account you can see four options: Check recent activity, Web browsing, Screen time and More options. All the options can be accessed by clicking on any of the links, so to begin with, click the Check recent activity option.


Microsoft
Store
Products
Support
Account
Your info
Privacy
Security
Rewards
Payment & billing
Services & subscriptions
Devices
Recent activity
Web browsing
Apps, games & media
Screen time
Purchases & spending
Find your child
Xbox privacy settings

anon.child.2000@mail.com

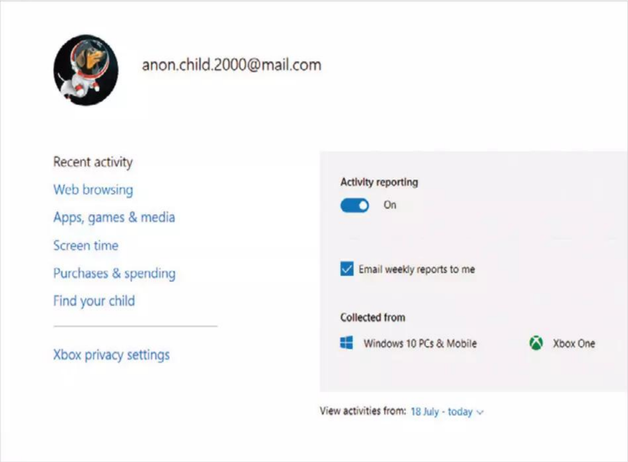
Activity reporting
Off

☑ Email weekly reports to me

Collected from
Windows 10 PCs & Mobile
Xbox One

A window into their digital life
Get recent activity reports on sites visited, apps used, games played and scr

STEP 3 Being a parent or guardian, you can set Activity Reporting for any of your Microsoft child accounts. Click on the Activity reporting slider to the On position; this will instantly block InPrivate browsing within Microsoft Edge and start to collect data on their online activity.


Recent activity
Web browsing
Apps, games & media
Screen time
Purchases & spending
Find your child
Xbox privacy settings

anon.child.2000@mail.com

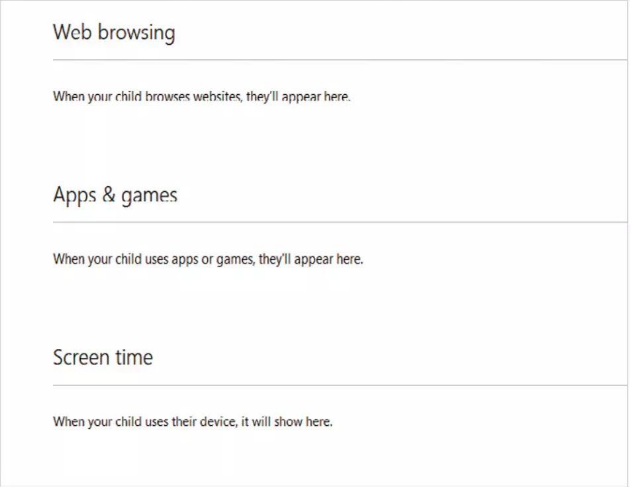
Activity reporting
On

☑ Email weekly reports to me

Collected from
Windows 10 PCs & Mobile
Xbox One

View activities from: 18 July - today

STEP 4 Under the Activity reporting, you can see sections for Web browsing, Apps & games and Screen time. To the right of each title are links to set up web access blocking, game and app blocking and so on. Click on the Turn on blocking link next to Web browsing to begin with.



Web browsing

When your child browses websites, they'll appear here.

Apps & games

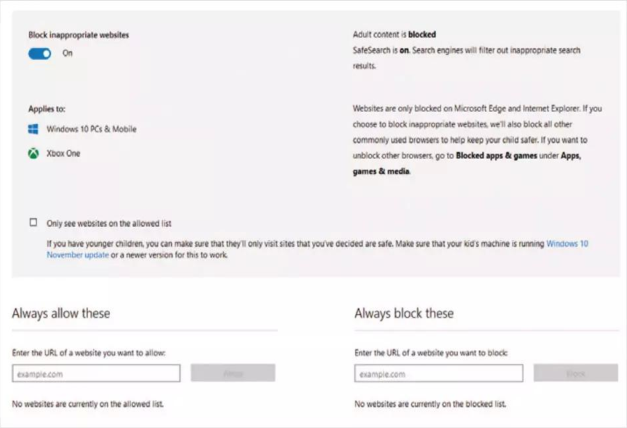
When your child uses apps or games, they'll appear here.

Screen time

When your child uses their device, it will show here.

STEP 5

Providing the child uses Microsoft Edge, you can set Windows 10 to automatically block any inappropriate websites by clicking the slider in the Turn on blocking link to the On position. By default, Microsoft will block all inappropriate sites but you can also specify an allow and block list of sites yourself.



Block inappropriate websites

On

Applies to:

Windows 10 PCs & Mobile

Xbox One

Adult content is **blocked**

SafeSearch is **on**. Search engines will filter out inappropriate search results.

Websites are only blocked on Microsoft Edge and Internet Explorer. If you choose to block inappropriate websites, we'll also block all other commonly used browsers to help keep your child safer. If you want to unblock other browsers, go to **Blocked apps & games** under **Apps, games & media**.

☐ Only see websites on the allowed list

If you have younger children, you can make sure that they'll only visit sites that you've decided are safe. Make sure that your kid's machine is running Windows 10 November update or a newer version for this to work.

Always allow these

Enter the URL of a website you want to allow:

example.com

No websites are currently on the allowed list.

Always block these

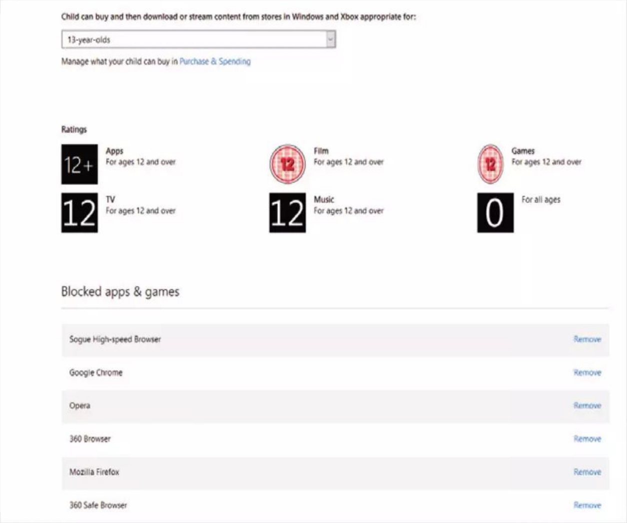
Enter the URL of a website you want to block:

example.com

No websites are currently on the blocked list.

STEP 6

Click on the back button in your browser to return to the previous page. Now click the Apps & games section and the Changing settings link. In here you can set age-specific restrictions on apps and games, as well as block certain programs from running, such as another browser, forcing them to use MS Edge instead.



Child can buy and then download or stream content from stores in Windows and Xbox appropriate for:

13-year-olds

Manage what your child can buy in Purchase & Spending

Ratings

12+ Apps For ages 12 and over

12 Film For ages 12 and over

12 Games For ages 12 and over

12 TV For ages 12 and over

12 Music For ages 12 and over

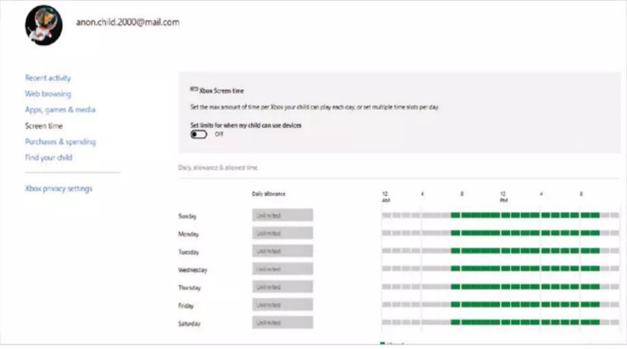
0 For all ages

Blocked apps & games

Sogue High-speed Browser	Remove
Google Chrome	Remove
Opera	Remove
360 Browser	Remove
Mozilla Firefox	Remove
360 Safe Browser	Remove

STEP 7

Screen time, found on the link to the left under the child's account name, will allow you to set time restrictions for the child. These restrictions will work for Windows 10 computers and devices, as well as Xbox consoles.



anon.child.2000@mail.com

- Recent activity
- Web browsing
- Apps, games & media
- Screen time
- Purchases & spending
- Find your child
- Xbox privacy settings

Xbox Screen time

Set the max amount of time per Xbox your child can play each day, or set multiple time slots per day.

Set limits for when my child can use devices

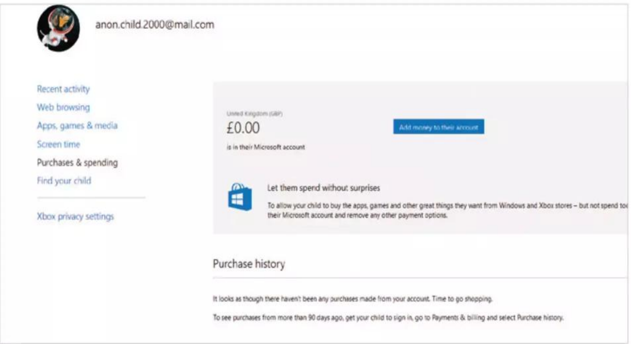
Off

Daily allowance & allowed time

	Daily allowance
Sunday	Unlimited
Monday	Unlimited
Tuesday	Unlimited
Wednesday	Unlimited
Thursday	Unlimited
Friday	Unlimited
Saturday	Unlimited

STEP 8

Purchases & spending is an interesting option and something which we'll be looking at in the next couple of pages. In here, you can specify a spending limit on the child's account as well as view their purchase history.



anon.child.2000@mail.com

- Recent activity
- Web browsing
- Apps, games & media
- Screen time
- Purchases & spending
- Find your child
- Xbox privacy settings

United Kingdom (GBP)

£0.00

is in their Microsoft account

Let them spend without surprises

To allow your child to buy the apps, games and other great things they want from Windows and Xbox stores – but not spend to
their Microsoft account and remove any other payment options.

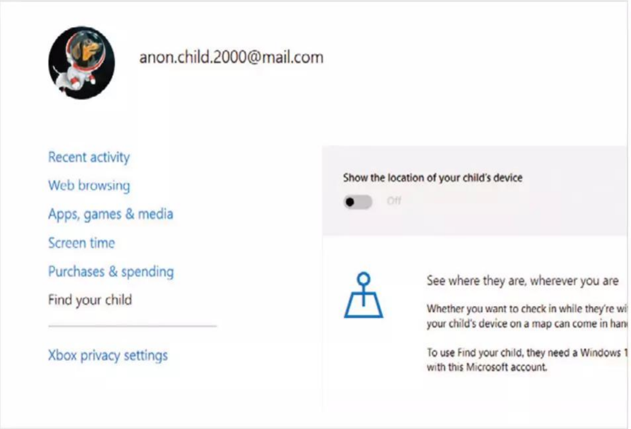
Purchase history

It looks as though there haven't been any purchases made from your account. Time to go shopping.

To see purchases from more than 90 days ago, get your child to sign in, go to Payments & billing and select Purchase history.

STEP 9

The Find your child setting works only with Windows 10 Mobile devices. With it, you're able to locate your child or rather their device, within just a few metres via a handy map. Useful for if they lose their device or just checking in on where they are.



anon.child.2000@mail.com

- Recent activity
- Web browsing
- Apps, games & media
- Screen time
- Purchases & spending
- Find your child
- Xbox privacy settings

Show the location of your child's device

Off

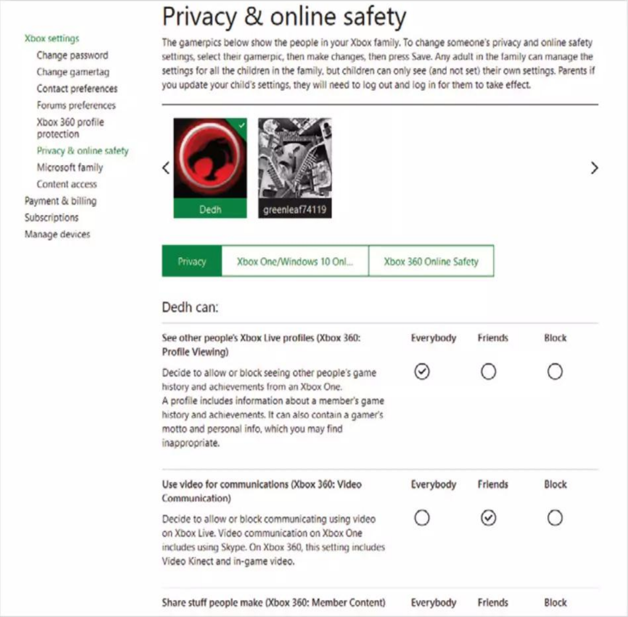
See where they are, wherever you are

Whether you want to check in while they're wi
your child's device on a map can come in han

To use Find your child, they need a Windows 1
with this Microsoft account.

STEP 10

If you own an Xbox One or Xbox 360, you're also able to set up any Xbox Privacy settings from within the Microsoft Family portal. You can specify video chat, viewing of profiles, sharing and other forms of communications from the console.



- Xbox settings
  - Change password
  - Change gamertag
  - Contact preferences
  - Forums preferences
  - Xbox 360 profile protection
  - Privacy & online safety
  - Microsoft family
  - Content access
- Payment & billing
- Subscriptions
- Manage devices

Privacy & online safety

The gamerpics below show the people in your Xbox family. To change someone's privacy and online safety settings, select their gamerpic, then make changes, then press Save. Any adult in the family can manage the settings for all the children in the family, but children can only see (and not set) their own settings. Parents if you update your child's settings, they will need to log out and log in for them to take effect.

Dedh can:

	Everybody	Friends	Block
See other people's Xbox Live profiles (Xbox 360: Profile Viewing) Decide to allow or block seeing other people's game history and achievements from an Xbox One. A profile includes information about a member's game history and achievements. It can also contain a gamer's motto and personal info, which you may find inappropriate.	☑	○	○
Use video for communications (Xbox 360: Video Communication) Decide to allow or block communicating using video on Xbox Live. Video communication on Xbox One includes using Skype. On Xbox 360, this setting includes Video Kinect and in-game video.	○	☑	○
Share stuff people make (Xbox 360: Member Content)	Everybody	Friends	Block

Problems with In-app Spending

The Internet is awash with horror stories from parents who have discovered that their child has spent an impressive sum on a game without their consent or knowledge; but, just how much of a problem is this in-app spending issue?

In-app spending is a modern scourge for parents, guardians and even the children and young people themselves. From the point of view of the parent or guardian, we have a child who enjoys playing a game, regardless of whether it's a mobile game, console game or triple-A rated PC game and we're more than happy to allow them to play the game without any restrictions, after all it's just a game, right? However, when those parents then receive the bill from their credit card company, or a call from the bank, that their account is now several hundred or even thousands of pounds lighter, that game has suddenly become the bane of their existence.

From the point of view of the child, they have an incredible and addictive game in front of them. They've put in the hours of game time to achieve a certain level but to get any further in the game, or to beat an end of the level boss or something, they need an extra push. That push can come in the form of more powerful spells, weaponry, armour or whatever else the game requires to boost the player's stats. To get hold of that equipment or bonus content, they need to purchase it from the in-game store. Some of the content costs just a few pounds but it soon lures them into the more expensive extras. Before they realise it, those few pound extras soon add up and the straw that breaks the camel's back is the expensive object that pushes them into the new levels, and causes the parents much angst.

The developers and creators of the game have their point of view too. These developers have spent many hours of coding, testing, re-coding and marketing to help launch their game. It's a painful, exhausting and often expensive process, so the company that launches the game will need to see some good returns if it still wants to continue in business and employing developers, testers and everyone else involved. All these people involved with the game need paying, so if they can top up the business with in-app purchases, added content and such, then why not.

Of course, that doesn't help the parent or guardian who is now looking at their vastly diminished bank account. What there must be is some form of middle ground, where the developers still get paid and the company can keep producing exciting and great games. Here the players get to reach the levels they want and continue playing the game and parents and guardians can safely leave their children to play the game and purchase an upgrade or two, without breaking the bank.

In light of events that hit the headlines, children spending thousands of pounds on purchasing virtual pets, virtual food, more lives etc., the main providers of mobile purchases, such as Apple, Google, Microsoft and so on, started to roll out levels of restrictions to help prevent overspending. These restrictions vary and have improved greatly in recent years; but initially they we're more centred around simple tips and advice for parents rather than the kind of spending restrictions we see today.

Of course, some of the problems also arise when the game in question is clearly a pay-to-win model. It's hardly fair for the young person to enjoy the game when they're continually beaten by those players who can afford to spend the money on extra lives, energy and so on. The pay to play model, on the other hand, requires the purchase of the app before it can even be played. Some experts argue that this is a better model but that's up for debate.

One of the main causes for excessive in-app spending is a child or young person being left alone with the device and game whilst the parent was logged into their own account. The account itself doesn't have any restrictions or password access to get into the online store, after all why would most people continually require password access to their own in-store account; or when the child knows the password and can easily access the store.

The child, left alone, could then go ahead and accept the message from the game that asked 'to continue, buy more apples' (or whatever), which in turn led them directly to the store to place the order in the basket without any kind of confirmation or message stating to check with an adult first.

Most of the time, when these sorts of scenarios occurred, the likes of Apple, Google and so on refunded the parents in question. From there, it became more difficult for a young person to go on an in-game spending spree with their parent's account.

There's a more controlled in-game and in-app spending focus these days but it's still not unheard of for a child to get a little carried away and purchase several hundred on some form of virtual extras for the game. Thankfully, we can combat a sizeable percentage of these cases with a little education and some much-needed tips, which we'll cover on the next couple of pages.

There are two main schools of thought on the Internet regarding the overspending in an app or game by a child. One view is that it's the fault of parents or guardians, letting their child on the game with unrestricted access to their mobile spending platform.

> ***Pay to Win***

The other view lies the blame at the feet of the developers and those who have created the app or game. Both have their valid points, and there's no right or wrong, but perhaps the blame lies equally with each.

Tips on How to Stop In-app Overspending

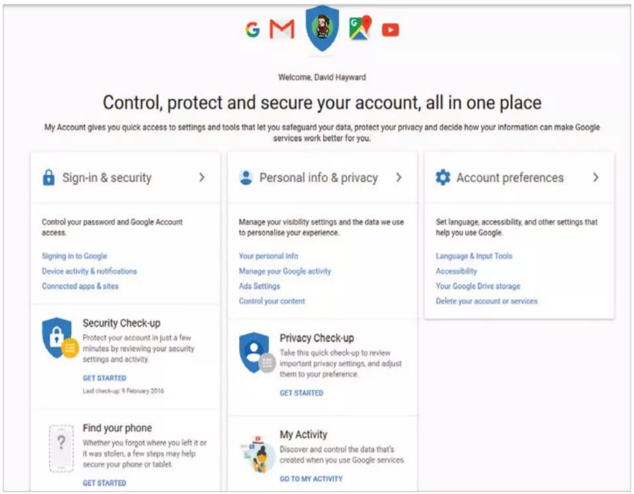
In-app overspending, as we've seen, is a concern for parents and guardians whenever their children use a phone, tablet, console or computer. However, there is a happy middle ground, where the kids can still enjoy their game and the parents needn't worry about in-app purchases.

10 Tips to Stop In-app Purchases

There's nothing wrong with spending money on a game, either to buy it in the first place or just to upgrade a part of it. What's needed though, is a little thought to combat overspending.

TIP 1 The main tip, and one that all child experts agree on, is simply don't leave your child alone with a device, console or computer whilst playing the game. Naturally it depends on the age of the child but essentially it's recommended never to leave a younger child alone, as that's when rogue spending can occur.

TIP 2 Set up their own account: using a child's account will dramatically cut down on any in-app overspending. Generally speaking, most children won't have access to a bank card to enter into the in-game shop or have access to the family bank details.



Welcome, David Hayward

Control, protect and secure your account, all in one place

My Account gives you quick access to settings and tools that let you safeguard your data, protect your privacy and decide how your information can make Google services work better for you.

Sign-in & security ›

Control your password and Google Account access.

Signing in to Google
Device activity & notifications
Connected apps & sites

Security Check-up

Protect your account in just a few minutes by reviewing your security settings and activity.

GET STARTED

Last check-up: 9 February 2016

Find your phone

Whether you forgot where you left it or it was stolen, a few steps may help secure your phone or tablet.

GET STARTED

Personal info & privacy ›

Manage your visibility settings and the data we use to personalise your experience.

Your personal info
Manage your Google activity
Ads Settings
Control your content

Privacy Check-up

Take this quick check-up to review important privacy settings, and adjust them to your preference.

GET STARTED

My Activity

Discover and control the data that's created when you use Google services

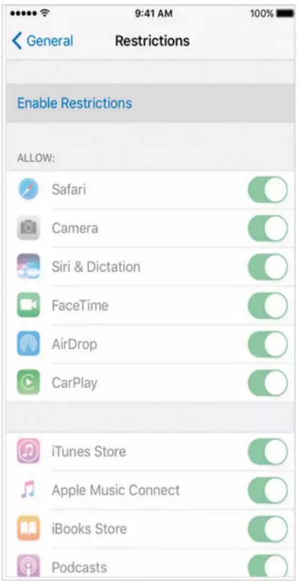
GO TO MY ACTIVITY

Account preferences ›

Set language, accessibility, and other settings that help you use Google.

Language & Input Tools
Accessibility
Your Google Drive storage
Delete your account or services

TIP 3 If you're using an iOS device, go to Settings > General > Restrictions and tap to enable the Restrictions. You can now create a passcode to lock out access to the iTunes Store, Safari and other Apple online portals, as well as other Apple apps.



9:41 AM 100%

‹ General Restrictions

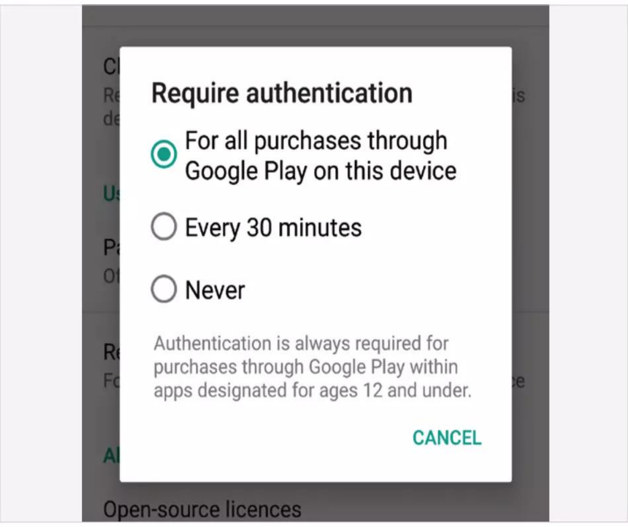
Enable Restrictions

ALLOW:

Safari ●
Camera ●
Siri & Dictation ●
FaceTime ●
AirDrop ●
CarPlay ●

iTunes Store ●
Apple Music Connect ●
iBooks Store ●
Podcasts ●

TIP 4 For Google devices, it's best to either never enter your banking details into Google Play or swipe in from the left whilst in the Play Store, choose Settings and tap the Require Authentication for Purchases option.



Require authentication

● For all purchases through Google Play on this device

○ Every 30 minutes

○ Never

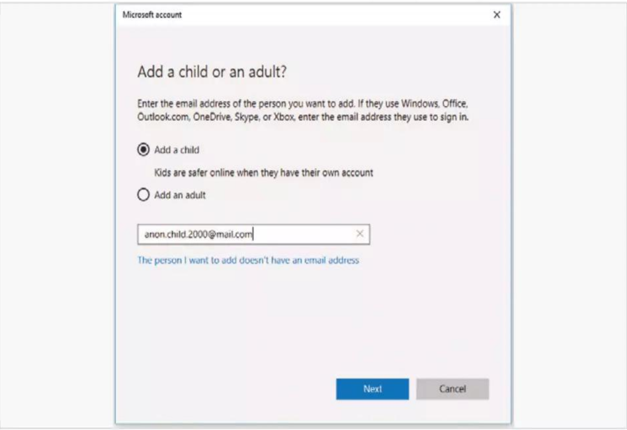
Authentication is always required for purchases through Google Play within apps designated for ages 12 and under.

CANCEL

Open-source licences

TIP 5

For Microsoft accounts, use the steps from our previous pages to create a child's account on your Windows 10 device; then use the Microsoft Family portal to restrict access to apps and spending.



Microsoft account

Add a child or an adult?

Enter the email address of the person you want to add. If they use Windows, Office, Outlook.com, OneDrive, Skype, or Xbox, enter the email address they use to sign in.

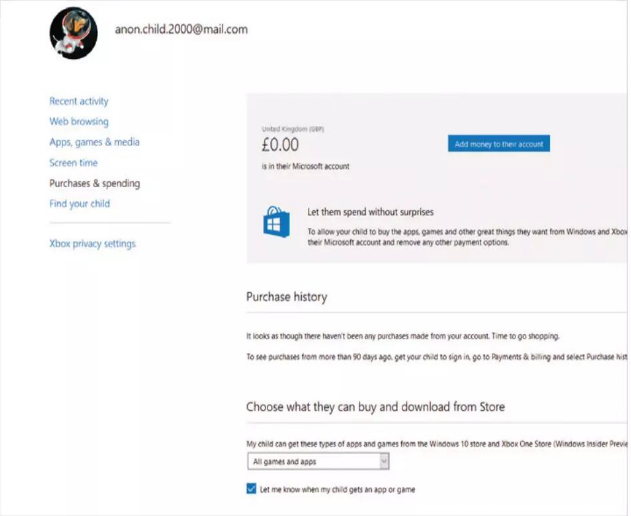
● Add a child
Kids are safer online when they have their own account
○ Add an adult

anon.child.2000@mail.com

The person I want to add doesn't have an email address

TIP 6

There's nothing wrong with spending money on a game, so why not consider setting up a limited amount of money on a Microsoft account. The child then has to then manage their own budget on in-app spending.



anon.child.2000@mail.com

United Kingdom (GBP)
£0.00
is in their Microsoft account

Let them spend without surprises
To allow your child to buy the apps, games and other great things they want from Windows and Xbox their Microsoft account and remove any other payment options.

Purchase history

It looks as though there haven't been any purchases made from your account. Time to go shopping.

To see purchases from more than 90 days ago, get your child to sign in, go to Payments & billing and select Purchase hist

Choose what they can buy and download from Store

My child can get these types of apps and games from the Windows 10 store and Xbox One Store (Windows Insider Previe
All games and apps
☑ Let me know when my child gets an app or game

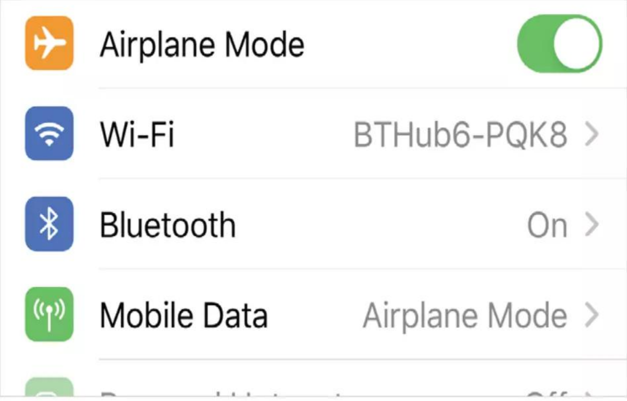
TIP 7

Similarly, consider using a gift card for iTunes or Google Play to allow any in-app spending. This way it's a more controlled purchasing environment and since the child is happy with the bonus app-extras, you're happy with the spending and the developer still gets paid. Everyone is happy with the outcome.

£10
Google play
MUSICMOVIESBOOKSAPPS&MORE
£25
£50

TIP 8

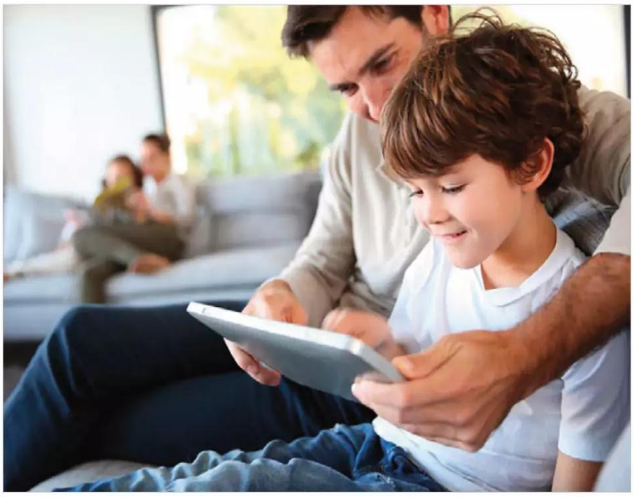
Enabling Airplane mode whilst the child is playing on the device stops any access to online services and thus the in-app or in-game stores. It's not ideal, and it can easily be deactivated, but for younger children it's a valid option.



Airplane Mode
Wi-Fi BTHub6-PQK8
Bluetooth On
Mobile Data Airplane Mode

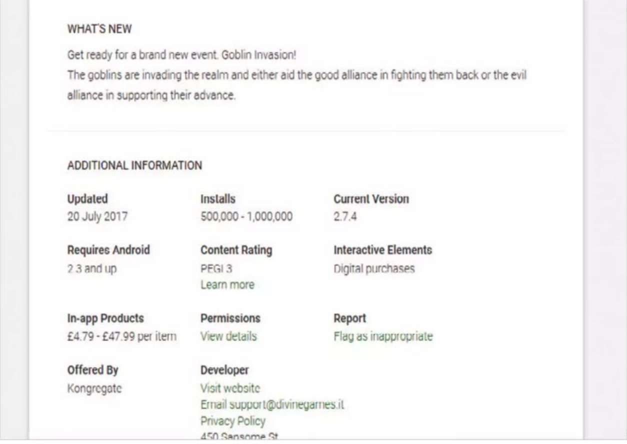
TIP 9

Talking to your children and taking the time to explain how in-app purchases work, and how bad it can be if they overspend, is a highly recommended option. Child experts state that the best policy to prevent overspending in apps and games is a little education.



TIP 10

Before your child downloads and installs a game or app, take a few moments to look through the app's information to see what, if any, in-app products are on offer. This section will usually inform you of how much money the in-app extras cost and you can then judge whether to allow the install or not.



WHAT'S NEW

Get ready for a brand new event. Goblin Invasion!
The goblins are invading the realm and either aid the good alliance in fighting them back or the evil alliance in supporting their advance.

ADDITIONAL INFORMATION

Updated 20 July 2017	**Installs** 500,000 - 1,000,000	**Current Version** 2.7.4
Requires Android 2.3 and up	**Content Rating** PEGI 3 Learn more	**Interactive Elements** Digital purchases
In-app Products £4.79 - £47.99 per item	**Permissions** View details	**Report** Flag as inappropriate
Offered By Kongregate	**Developer** Visit website Email support@divinegames.it Privacy Policy 450 Sansome St	

Online Child Safety at School

Whilst you're doing everything you can at home to ensure your child is safe when online, what happens when they're out of the protection of your home network? Schools are up against as much, if not more, online safety issues as parents.

How does your child's school provide online safety? What tools and procedures do they use? What government backed schemes are available for them?

> **Safer Schooling**

What's their policy on cyber bullying and what's the process should anything inappropriate ever make its way into the school's network?

Most of those questions are dependent on the school itself and what policies it's created in collaboration with the council, local government, parents, teachers and governing body. In the UK, the UKCCIS (UK Council for Child Internet Safety) has drawn up and developed a guide for school governors to follow, to help governing boards support their school leaders in keeping children safe online. It's an interesting six-page document and further reading can be found with the accompanying Sexting in Schools and Colleges 50-page guidance document. You can find both at *https://www.gov.uk/government/groups/uk-council-for-child-Internet-safety-ukccis*.

From 22 December 2015, the Department for Education put in place strengthened measures to help protect children from harm online, which included cyber bullying, access to pornography and the risks involved with radicalisation. These measures enforced schools to improve or implement better filters and monitoring systems, guides on social media and good practise and the teaching of online threats and the issues surrounding it.

This safeguarding of students through education is one of the best forms of introducing a heightened level of Internet safety amongst young people. Parents and guardians can rant and rave about Internet safety until they are blue in the face but when it comes as part of a lesson in the school, the message is considered to be delivered with a more meaningful impact. In classes, students are taught what Internet use is acceptable, and what isn't and given clear objectives for Internet use. The school is also capable and often required to consult with outside child protection agencies, bringing in experts to help further the student's understanding of the dangers and risks of the Internet, social media and all forms of digital behaviour.

Beyond the classroom talks and conversations, schools employ an assortment of advanced monitoring tools and filters. The school's expert IT staff will already use a range of network level security features found only in the server versions of Windows, or Linux. These features will restrict the students' activities, whilst still offering them access to much needed resources both internally and externally on the Internet. If your child is new to the school, take a moment to ask if you can speak to the head of the school's IT or IT manager and ask them what they use and do to set limits and restrictions on local and Internet resources. Most of the techniques used are quite fascinating, even from a non-technical point of view, and often can be applied to a lesser, but just as effective, degree on the home network.

In addition to protection on the network level, the IT team will also implement a range of site-level Net Nanny-like programs. They may only use a single program, installed on a server to manage each workstation or they may use several programs to manage each student's account; monitoring sites visited and providing blocks for sites that are deemed inappropriate. Another element to consider with a schools' IT is the use of its available bandwidth. With hundreds, often thousands, of devices and computers attached to the school network it can at times become a little slow, as there's limited bandwidth. A school's IT team therefore must also decide whether or not to block access to sites that will cause a strain on the bandwidth, such as online game sites or media streaming. Whilst the students may be blocked from such sites, the teachers are usually unrestricted, for teaching purposes.

These filters, blocked sites and bandwidth monitoring techniques all add up to make an effective protection net around the school's IT infrastructure. It's important to understand, from a parent's point of view, the amount of work needed to achieve such a high degree of online safety and that it can become quite expensive once you factor in licensed software. Where you might have purchased a child filtering product, and employed some of the security techniques we've used in this book, a school IT system needs to do all that times a thousand-plus for each student, computer and device.

Nevertheless, a school's online safety requirements are exceptionally more advanced than you have at home. With this in mind, your child is less likely to experience any online risks when at school than at home. However, it's always best to take the time to make an appointment with the school to ask what they're doing to ensure online safety.

Where to Find Help with Online Child Safety

The tips and features throughout this book will help you build a better understanding of security and online safety, with special reference to online child safety. If you want to know more though, or you have some pressing questions that need answering, here are some places to check out.

Help is at Hand

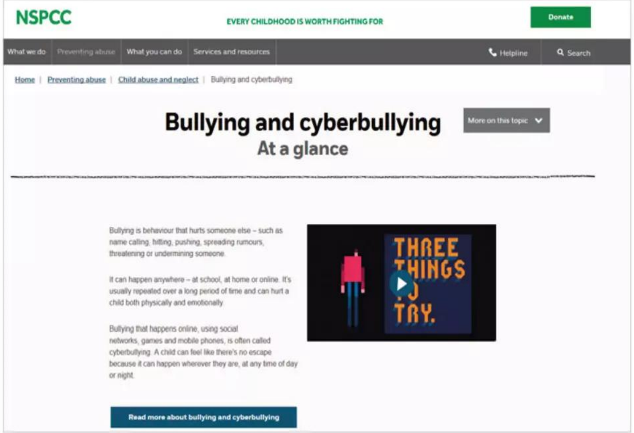
For more information, expert advice from child care professionals and more tips on how to protect your child when online, here are ten sites to bookmark and consider.

TIP 1 If you'd rather contact a professional child care expert, person to person, then consider contacting your local doctor's surgery and asking for a list of contact details of the child counsellors in the area. Most surgeries will have all the relevant information to hand for you.

Doctors
Surgery

TIP 2 Your child's teachers and school welfare officers will have an excellent understanding of how to help keep your child safe when online. They can answer your questions or at least help point you in the right direction.

TIP 3 Regardless of where you are in the world, the UK's NSPCC website contains invaluable information regarding child safety, especially online child safety. You can find the main site at **https://www.nspcc.org.uk/**, with access to services and resources.


NSPCC
EVERY CHILDHOOD IS WORTH FIGHTING FOR
Donate
What we do
Preventing abuse
What you can do
Services and resources
Helpline
Search
Home | Preventing abuse | Child abuse and neglect | Bullying and cyberbullying
More on this topic
THREE THINGS TO TRY.
Read more about bullying and cyberbullying

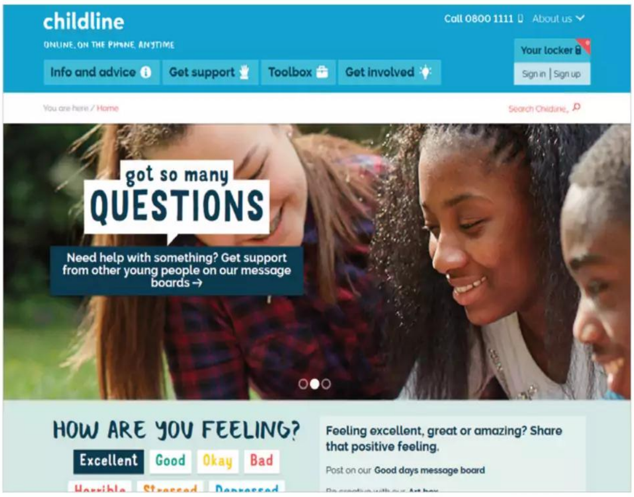
Bullying and cyberbullying
At a glance

Bullying is behaviour that hurts someone else – such as name calling, hitting, pushing, spreading rumours, threatening or undermining someone.

It can happen anywhere – at school, at home or online. It's usually repeated over a long period of time and can hurt a child both physically and emotionally.

Bullying that happens online, using social networks, games and mobile phones, is often called cyberbullying. A child can feel like there's no escape because it can happen wherever they are, at any time of day or night.

TIP 4 In addition to the NSPCC, the UK's Childline is also an exceptional resource that contains a wealth of information and support for families, parents, guardians and children. There's a superb online safety section too. You can find Childline at **https://www.childline.org.uk/**.

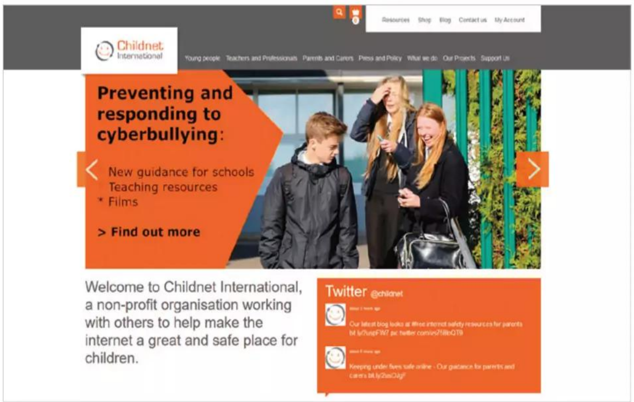

childline
ONLINE, ON THE PHONE, ANYTIME
Call 0800 1111
About us
Your locker
Sign in | Sign up
Info and advice
Get support
Toolbox
Get involved
You are here / Home
Search Childline
got so many QUESTIONS
Need help with something? Get support from other young people on our message boards →
HOW ARE YOU FEELING?
Excellent
Good
Okay
Bad

Feeling excellent, great or amazing? Share that positive feeling.

Post on our Good days message board

TIP 5

Childnet International is a site dedicated to young people, children, teachers and professionals, parents and carers. There's a ton of resources and support available through the site and plenty of advice about online child safety. Find it at **http://www.childnet.com/**.


Resources
Shop
Blog
Contact us
My Account
Childnet International
Young people
Teachers and Professionals
Parents and Carers
Press and Policy
What we do
Our Projects
Support Us
> Find out more
Twitter @childnet

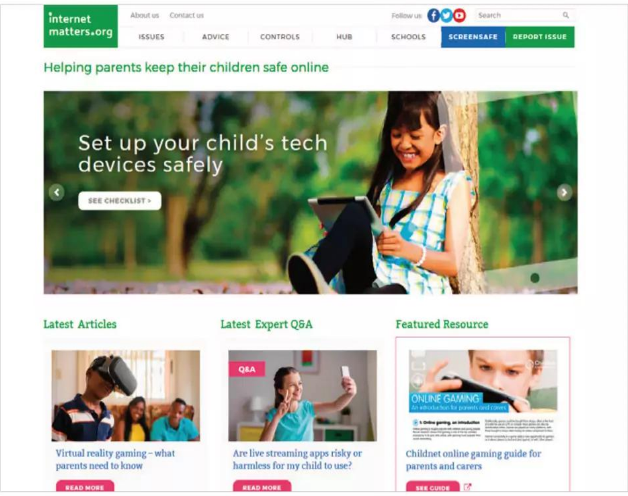
Preventing and responding to cyberbullying:

New guidance for schools
Teaching resources
* Films

Welcome to Childnet International, a non-profit organisation working with others to help make the internet a great and safe place for children.

TIP 6

Internet Matters features articles, advice, support, guidelines and tips on how to protect your children better when online. There are plenty of resources to hand for children at preschool, all the way up to teenagers at college. It's at **https://www.Internetmatters.org/**.


internet matters.org
About us
Contact us
Follow us
Search
ISSUES
ADVICE
CONTROLS
HUB
SCHOOLS
SCREENSAFE
REPORT ISSUE
SEE CHECKLIST >
Q&A
ONLINE GAMING
READ MORE
READ MORE
SEE GUIDE

Helping parents keep their children safe online

Set up your child's tech devices safely

Latest Articles

Virtual reality gaming – what parents need to know

Latest Expert Q&A

Are live streaming apps risky or harmless for my child to use?

Featured Resource

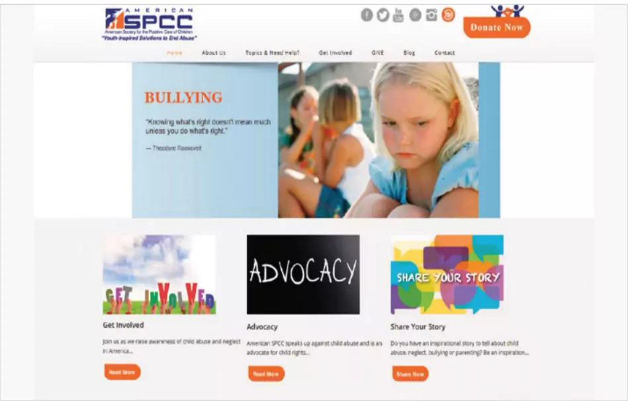
Childnet online gaming guide for parents and carers

TIP 7

To expand on the first entry in our list, local support groups are an ideal source of information and tips. Other parents and guardians going through the same considerations as yourself may well be more than happy to share any tips they have.

TIP 8

The American SPCC (Society for the Positive Care of Children) is yet another superb site that details advice on cyber bullying amongst other child protection issues. There's also a list of recommended books for you to look up. You can find the ASPCC at **http://americanspcc.org/**.


AMERICAN SPCC
"Youth Inspired Solutions to End Abuse"
Donate Now
About Us
Topics & Need Help?
Get Involved
GIVE
Blog
Contact
GET INVOLVED
ADVOCACY
SHARE YOUR STORY

BULLYING

"Knowing what's right doesn't mean much unless you do what's right."

— Theodore Roosevelt

Get Involved

Join us as we raise awareness of child abuse and neglect in America...

Advocacy

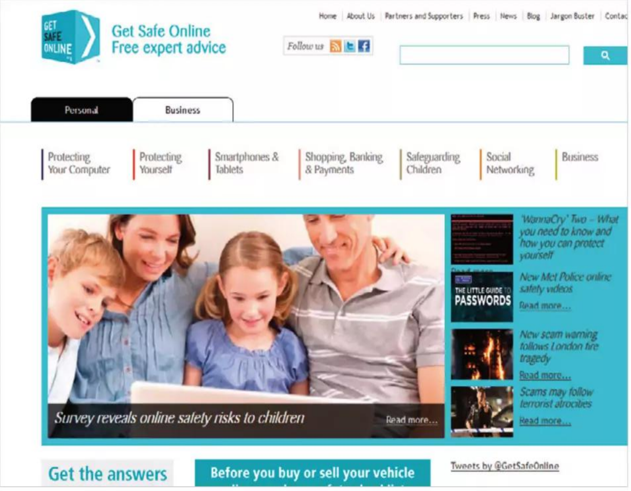
American SPCC speaks up against child abuse and is an advocate for child rights...

Share Your Story

Do you have an inspirational story to tell about child abuse, neglect, bullying or parenting? Be an inspiration...

TIP 9

There are some excellent resources available on the Get Safe Online website. Here you can find tips, advice and tutorials covering nearly all aspects of online child safety, including emphasis on mobile devices; there's plenty to get through. You can find it all at **https://www.getsafeonline.org/**.


GET SAFE ONLINE
Get Safe Online
Free expert advice
Home
About Us
Partners and Supporters
Press
News
Blog
Jargon Buster
Follow us
Personal
Business
Protecting Your Computer
Protecting Yourself
Smartphones & Tablets
Shopping, Banking & Payments
Safeguarding Children
Social Networking
Business
THE LITTLE GUIDE TO PASSWORDS
Read more...
Read more...
Read more...
Read more...
Tweets by @GetSafeOnline

Survey reveals online safety risks to children

'WannaCry' Two – What you need to know and how you can protect yourself

New Met Police online safety videos

New scam warning follows London fire tragedy

Scams may follow terrorist atrocities

Get the answers

Before you buy or sell your vehicle

TIP 10

Finally, consider checking out the website of, or visiting, the local police station for more information on online safety. The police have information on area professionals and child safety experts as well as further information on what to do if your child is the victim of an online threat.

POLICE
POLICE

What the Experts Say

Our next generation is heading into an ever increasingly connected, digital world. What we perceive as threats now will certainly change in a decade's time, as the technology surrounding us evolves and becomes even more integrated. What will remain important though, is online safety.

> *“We've gathered together quotes and asked child safety and security experts to have their say on the matter of online safety; as a result, here are ten examples from the professionals”*

> “Start discussing online safety at an early age.”

David Emm, senior security researcher at Internet security company Kaspersky Lab.

> “Talking to your child openly and regularly is the best way to help keep them safe online.”

NSPCC, Keeping Children Safe Online.

> “Follow the same rules you would follow in the real world.”

Darren Anstee, director of solutions architects at network security company Arbor Networks.

“Think before you post. Don’t upload or share anything you wouldn’t want your parents, teachers or friends seeing. Once you press send, it is no longer private. You can’t be sure who will end up seeing it”

Childline.

“If you wouldn’t do it face to face, don’t do it online.”

Shelagh McManus, online safety advocate for security software Norton by Symantec.

“Ask them about how they stay safe online. What tips do they have for you, where did they learn them and what is OK and not OK to share”

Childnet, Staying Safe Online.

“You might find it helpful to start with a family discussion, to set boundaries and agree what’s appropriate.”

NSPCC, Keeping Children Safe Online.

“Don’t be pressured to give your number out. If someone is pressuring you into giving them your number, tell someone about it such as a teacher or parent.”

Childline.

“Set and monitor limits for the amount of daily or weekly time your children spend online gaming.”

Get Safe Online, Safeguarding Children, Gaming.

“Don’t meet people you don’t know. Even if you get on with them online, you never know who they really are.”

Childline.

Glossary of Terms

The bewildering world of technological terms is often difficult even for experts to navigate without becoming slightly confused and we could easily dedicate an entire book just to the glossary. However, here are some of the more important terms from the world of digital security and safety.

Digital Security A-Z

Digital security and safety terms are often as clear as mud. Use this glossary whenever you come across a term you don't understand.

A

Access Control: A term used to ensure that resources are only granted to users who are entitled to them.

Active Content: Code that's embedded in a web site. When the site is accessed the code is automatically downloaded and executed.

Advanced Encryption Standard (AES): An encryption standard designed to specify an unclassified, publicly disclosed, symmetric encryption algorithm.

Asymmetric Cryptography: Public key cryptography, where algorithms use a pair of keys, one public and one private, to unlock the content protected by the encryption.

Authentication: Used by systems to confirm the identity of a user.

B

Backdoor: A tool used by hackers or system security experts to access a computer system or network, bypassing the system's usual security mechanisms.

Bandwidth: The limited amount of communications data that any channel is capable of sending or receiving in a specific time.

Biometrics: A security measure that uses physical characteristics to authenticate a user's access to a system.

Boot Sector Virus: A virus that can affect a computer as it boots, before the operating system has even loaded.

Botnet: A large number of Internet connected, infected computers that are used to flood a network or send spam message to the rest of the Internet.

Brute Force: A hacking technique that uses all possible password combinations one at a time in order to gain access to a user account or system.

C

Cipher: A cryptographic algorithm used in the encryption and decryption process.

Cookie: A file used to store information about a website that can be read should the user ever visit the site again.

Cyber Attack: An attack on a system using malware to compromise its security. Usually in order to gain access to steal information or demand a ransom.

Cyber Bullying: When an individual, or group of individuals, threaten or post negative and derogatory messages or doctored images of someone online.

D

Data Encryption Standard (DES): A popular method of data encryption using a private (secret) key. There are 72,000,000,000,000,000 (72 quadrillion) or more possible encryption keys that can be used.

Decryption: The process of transforming an encrypted message into its original text form.

Demilitarised Zone (DMZ): A demilitarised zone (DMZ) or perimeter network is a network area (a subnetwork) that sits between an organisation's internal network and an external network, usually the Internet. DMZ's help to enable the layered security model in that they provide subnetwork segmentation based on security requirements or policy. DMZ's provide either a transit mechanism from a secure source to an insecure destination or from an insecure source to a more secure destination.

Denial of Service (DoS): Prevention of authorised access to a system or network.

Disaster Recovery Plan (DRP): A plan of action used to restore systems in the event of a disaster.

Distributed Denial of Service (DDoS): A type of DoS attack using multiple attacking systems to amplify the amount of network traffic, thereby flooding and swamping the target systems or networks.

Domain Name System (DNS): The domain name system (DNS) is the way that Internet domain names are located and translated into Internet Protocol addresses. A domain name is a meaningful and easy to remember 'handle' for an Internet address.

E

Encryption: The process of securing data by transforming it into something unreadable using cryptographic means.

Ethernet: Communication architecture for wired local area networks.

F

Fingerprinting: Used by hackers and security experts to send packets to a system in order to see how it responds, usually to determine the operating system and security measures.

Firewall: A hardware or software layer designed to prevent unauthorised access to or from a computer or network to another computer or network.

Flooding: A malware attack that causes an eventual failure of a system by bombarding it with a continuous stream of data.

G

Gateway: A network point that acts as the door into another network.

H

Hacker: Someone who violates or circumvents a computer security measure. Can be used for malicious purposes or legitimately to test a system's vulnerabilities.

HTTP: Hypertext Transfer Protocol, the protocol used by the World Wide Web (Internet) that defines how messages are sent, received and read by browsers and other connected software layers.

HTTPS: Hypertext Transfer Protocol Secure, an encrypted and far more secure version of HTTP.

I

Internet Protocol Address (IP): A standard used by servers and machines to connect to each other and form an individual identity for each connected device.

Internet Service Provider (ISP): A company that provides Internet access to businesses and residential addresses.

IP Spoofing: A form of attack where a device provides a false IP address to a server or network.

K

Key Logger: A type of malware that can record key presses as a text file and send that file to a remote source. Once obtained, the hacker can then see what keys you've pressed.

L

Local Area Network (LAN): Communications network linking multiple devices in a defined, limited location, such as a home or office.

Logic Bomb: A type of malware that's dormant until a predefined time when it explodes and runs or injects malicious code into a system.

M

Malicious Code: Software that's designed to circumvent security measures and gain unauthorised access to a system.

Malware: A generic term to describe different types of malicious code.

N

Network: A group of linked computers or devices that can share resources and communicate with each other.

P

Password: A secret security measure used to access a protected resource and authenticate access.

Phishing: A method used by cyber criminals to obtain information from a user by baiting them with fake emails or messages.

PIN: Personal Identification Number, used as a form of authentication access to a system, resource or user account.

R

Ransomware: A type of malware that locks, or encrypts, all files on a system until a ransom is paid and the unlock code is entered.

Rootkit: A set of tools used by a hacker to mask their intrusion and obtain administrator access to a system.

S

Sandbox: A system architecture designed to test code in a secure and safe environment without it affecting the host system.

Spoofing: An attempt to gain unauthorised access.

Spyware: A type of malware that spies on a user's activities or system and reports back to a remote system.

T

Trojan Horse: A type of malware designed as a useful program but in reality hides some malicious code.

Two-Factor Authentication: Authorisation of access to a system or resource through a username/password combination as well as another form of authorisation, such as a PIN code.

V

Virus: A type of malware designed for multiple purposes to spread and infect as many computer systems as possible. Usually destructive but can be used to grind a system to a halt by using up all of its available resources.

VPN: Virtual Private Network, a secure tunnel between two systems using advanced encryption methods to protect the communications between systems.

W

Wi-Fi: A wireless network standard between connected systems.

Worm: A type of malware that can replicate itself and spread through other systems consuming resources and contents destructively.

Z

Zero Day: Described as the day a new security vulnerability is discovered, one that has no fix or patch yet to stop it.

Zombie(s): A computer that's infected with malware and connected to a network or the Internet and used to spread its infection to other computers. Used also to describe an attack on other systems by hoards of zombie computers.

Black Dog Media

Master Your Tech

From Beginner to Expert

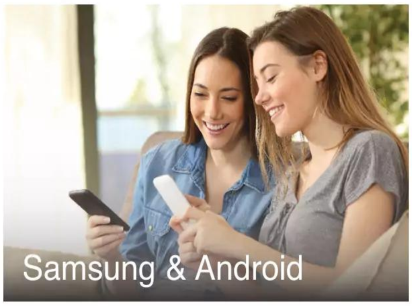
To continue learning more about your tech visit us at:

www.bdmpublications.com

FREE Tech Guides

Apple iPhone, iPad, Mac, MacBook & Watch

PC & Windows 10


Samsung & Android

Photography, Photoshop & Lightroom

Coding Python, Raspberry Pi & Linux

EXCLUSIVE Offers on our Tech Guidebooks

- Print & digital editions
- Featuring the very latest updates
- Step-by-step tutorials and guides
- Created by BDM experts

Check out our latest titles today!

The iOS 14 iPhone GuideBook
Raspberry Pi Tips, Tricks & Fixes
Coding for Beginners
The python Coding Manual
The iPad GuideBook 14
Windows 10 The Complete Guide
Photography The Beginners' Guide
The Adobe Photoshop Manual

BDM's Ultimate Photoshop

bdmpublications.com/ultimate-photoshop

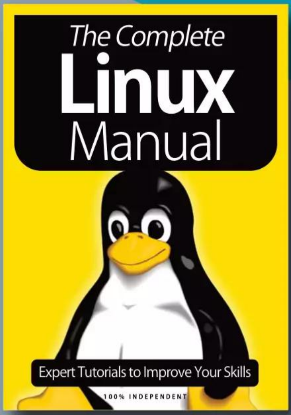
Buy our Photoshop guides and download tutorial images for free! *Simply sign up and get creative.*

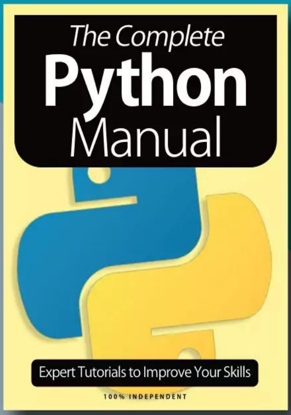
PLUS

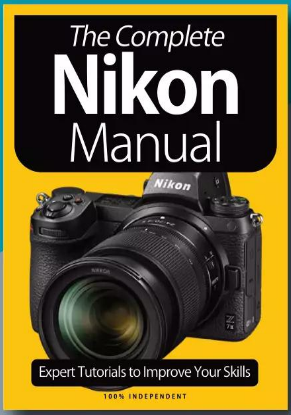
SPECIAL DEALS and Bonus Content

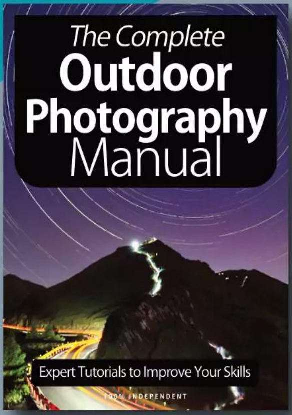
Sign up to our monthly newsletter and get the latest updates, offers and news from BDM. We are here to help you Master Your Tech!

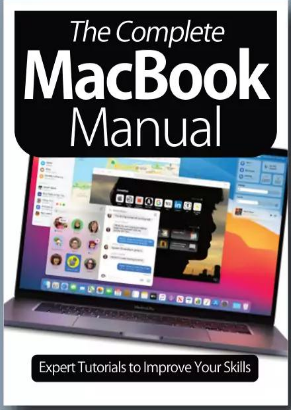
Discover more of our guides today...

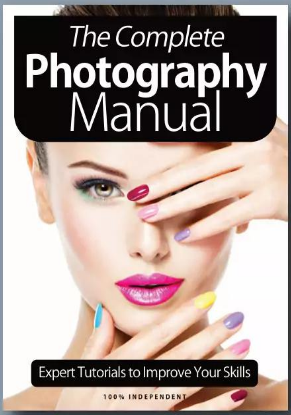

The Complete
Linux
Manual
Expert Tutorials to Improve Your Skills
100% INDEPENDENT

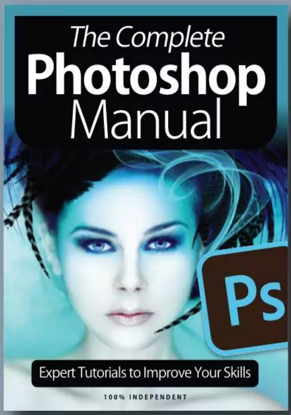

The Complete
Python
Manual
Expert Tutorials to Improve Your Skills
100% INDEPENDENT

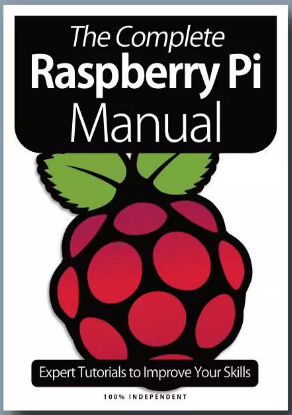

The Complete
Nikon
Manual
Nikon
Expert Tutorials to Improve Your Skills
100% INDEPENDENT

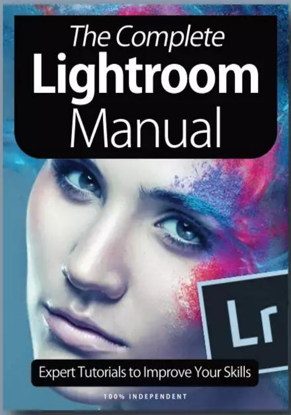

The Complete
Outdoor
Photography
Manual
Expert Tutorials to Improve Your Skills
100% INDEPENDENT

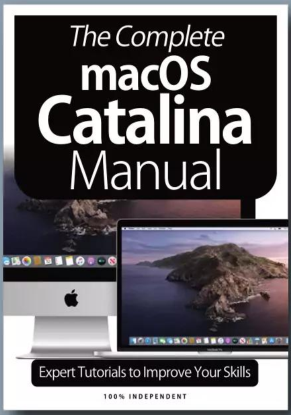

The Complete
MacBook
Manual
Expert Tutorials to Improve Your Skills


The Complete
Photography
Manual
Expert Tutorials to Improve Your Skills
100% INDEPENDENT

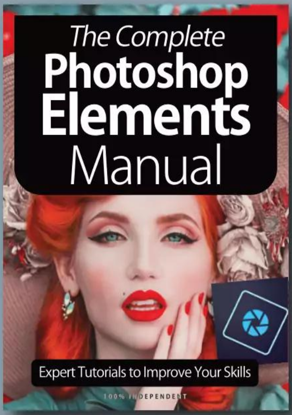

The Complete
Photoshop
Manual
Ps
Expert Tutorials to Improve Your Skills
100% INDEPENDENT


The Complete
Raspberry Pi
Manual
Expert Tutorials to Improve Your Skills
100% INDEPENDENT

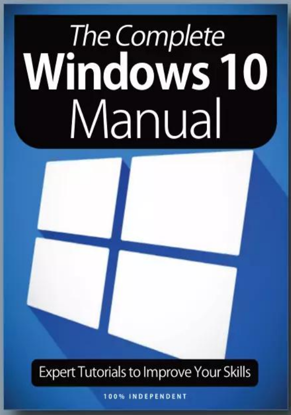

The Complete
Lightroom
Manual
Lr
Expert Tutorials to Improve Your Skills
100% INDEPENDENT

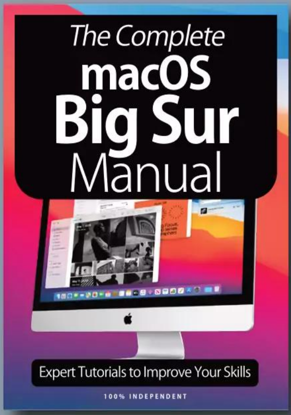

The Complete
macOS
Catalina
Manual
Expert Tutorials to Improve Your Skills
100% INDEPENDENT

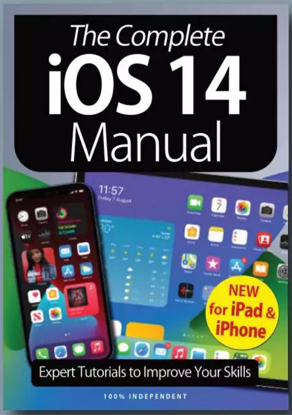
The Complete
Python &
C++
Manual
Expert Tutorials to Improve Your Skills
100% INDEPENDENT


The Complete
Photoshop
Elements
Manual
Expert Tutorials to Improve Your Skills
100% INDEPENDENT

The Complete
Samsung
Galaxy
Manual
Expert Tutorials to Improve Your Skills
100% INDEPENDENT


The Complete
Windows 10
Manual
Expert Tutorials to Improve Your Skills
100% INDEPENDENT


The Complete
macOS
Big Sur
Manual
Expert Tutorials to Improve Your Skills
100% INDEPENDENT


The Complete
iOS 14
Manual
NEW
for iPad & iPhone
Expert Tutorials to Improve Your Skills
100% INDEPENDENT